

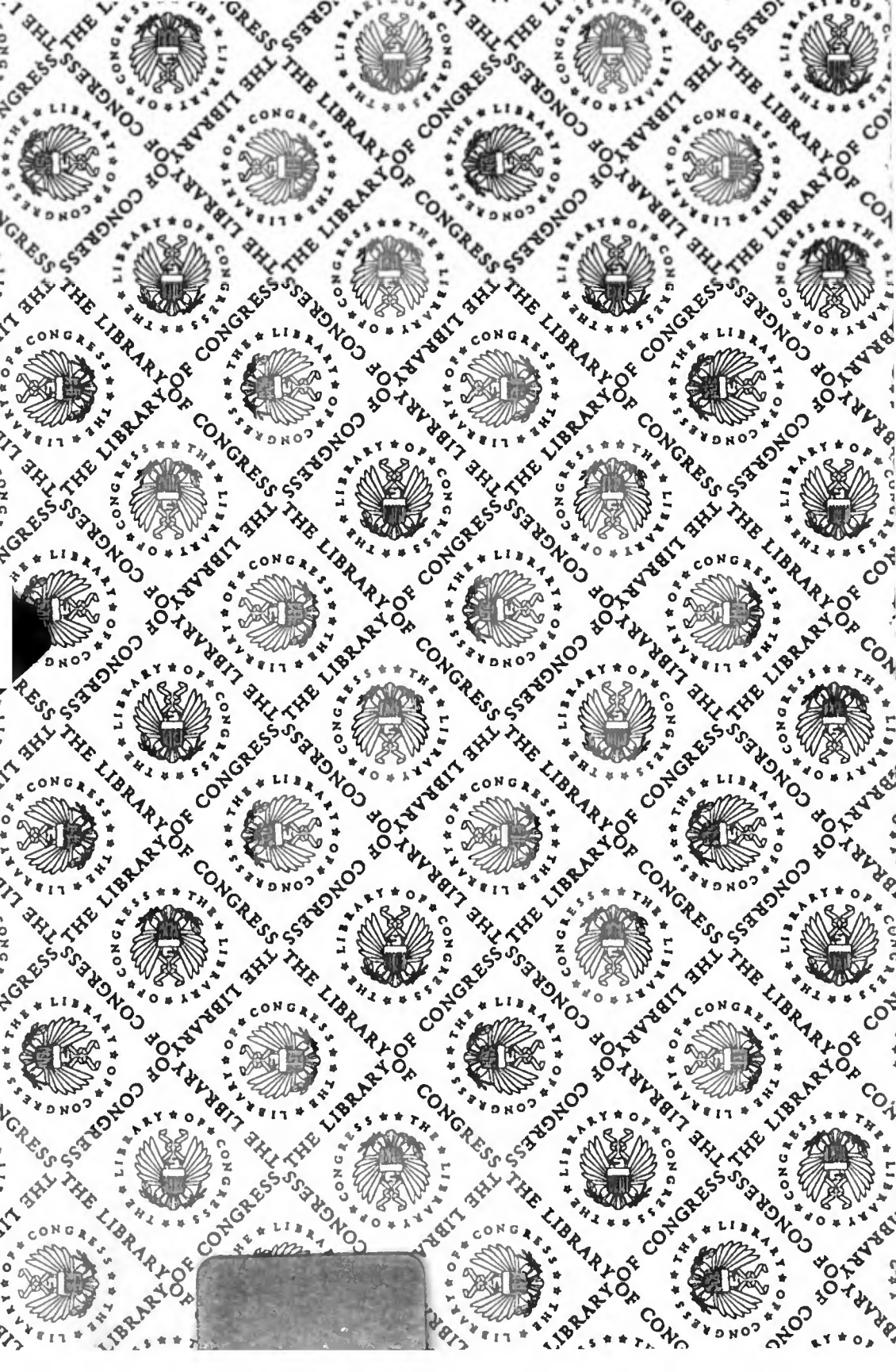
LL

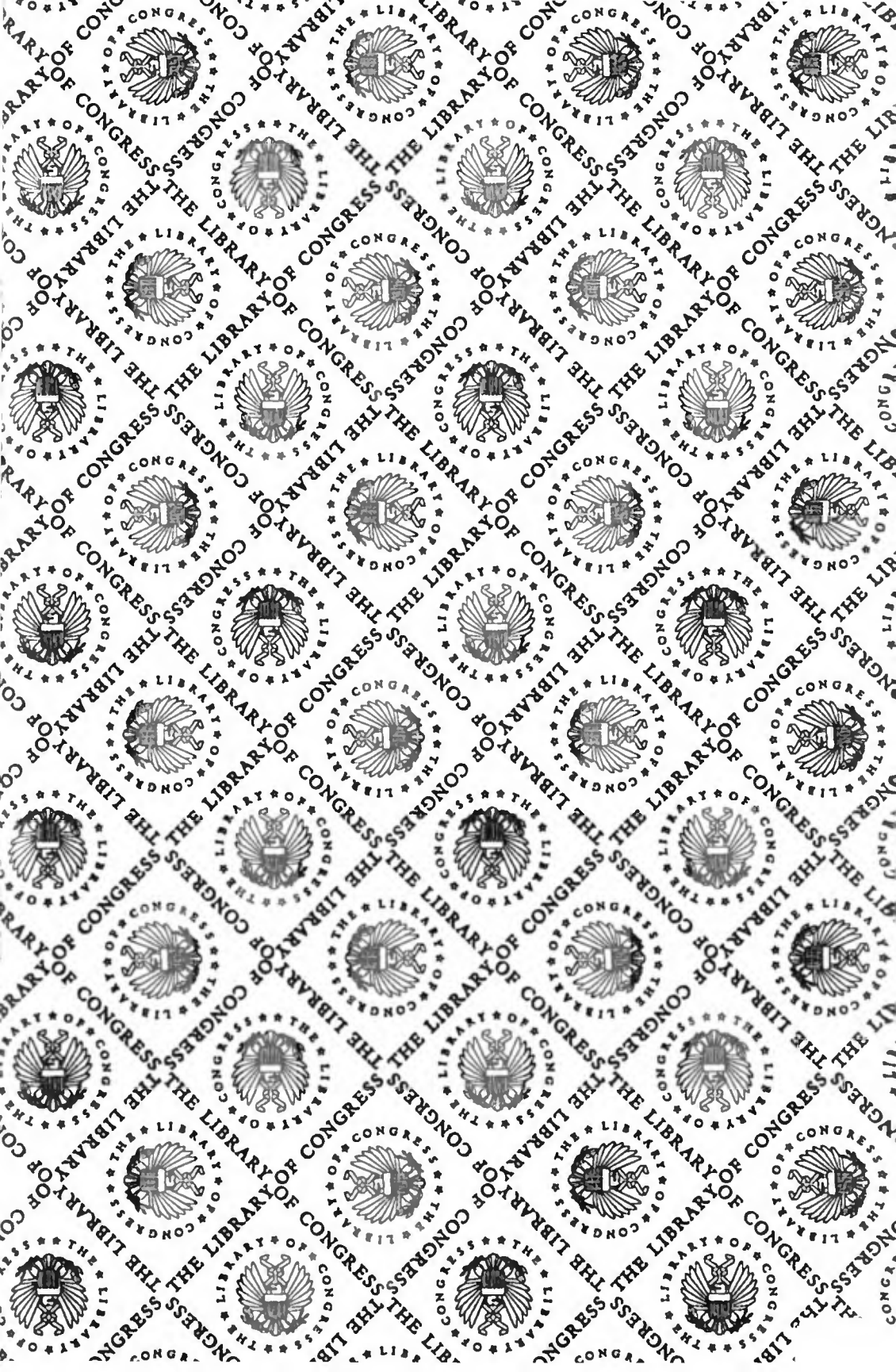
KF 27

.J857

~~2000~~f

Copy 1





COMMITTEE ON THE JUDICIARY

HENRY J. HYDE, *Illinois, Chairman*

F. JAMES SENSENBRENNER, JR.,
Wisconsin
BILL McCOLLUM, Florida
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR S. SMITH, Texas
ELTON GALLEGLEY, California
CHARLES T. CANADY, Florida
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
BOB BARR, Georgia
WILLIAM L. JENKINS, Tennessee
ASA HUTCHINSON, Arkansas
EDWARD A. PEASE, Indiana
CHRIS CANNON, Utah
JAMES E. ROGAN, California
LINDSEY O. GRAHAM, South Carolina
MARY BONO, California
SPENCER BACHUS, Alabama
JOE SCARBOROUGH, Florida
DAVID VITTER, Louisiana

JOHN CONYERS, JR., Michigan
BARNEY FRANK, Massachusetts
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York

THOMAS E. MOONEY, SR., *General Counsel-Chief of Staff*
JULIAN EPSTEIN, *Minority Chief Counsel and Staff Director*

SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY

HOWARD COBLE, *North Carolina, Chairman*

F. JAMES SENSENBRENNER, JR.,
Wisconsin
ELTON GALLEGLEY, California
BOB GOODLATTE, Virginia
WILLIAM L. JENKINS, Tennessee
EDWARD A. PEASE, Indiana
CHRIS CANNON, Utah
JAMES E. ROGAN, California
MARY BONO, California

HOWARD L. BERMAN, California
JOHN CONYERS, JR., Michigan
RICK BOUCHER, Virginia
ZOE LOFGREN, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida

BLAINE MERRITT, *Chief Counsel*
VINCE GARLOCK, *Counsel*
DEBBIE K. LAMAN, *Counsel*
CHRIS J. KATOPIS, *Counsel*
ALEC FRENCH, *Minority Counsel*
EUNICE GOLDRING, *Staff Assistant*



PRIVACY AND ELECTRONIC COMMUNICATIONS

HEARING
BEFORE THE
SUBCOMMITTEE ON COURTS AND INTELLECTUAL
PROPERTY
OF THE
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTH CONGRESS
SECOND SESSION

U.S. HOUSE OF REPRESENTATIVES
MAY 14, 2000

MAY 18, 2000

Serial No. 86



Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2000

65-439

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

This errata sheet is being assigned because the serial number was incorrect in the original printing.

The number assigned to this hearing is Serial Number 87.

KF27
J857
2000F
copy 1
LL

CONTENTS

HEARING DATE

May 18, 2000	Page 1
--------------------	-----------

OPENING STATEMENT

Coble, Hon. Howard, a Representative in Congress from the State of North Carolina, and chairman, Subcommittee on Courts and Intellectual Property	1
---	---

WITNESSES

Bernstein, Joan Z., Director, Bureau of Consumer Protection, Federal Trade Commission	15
Bruening, Paula J., director of compliance and policy, TRUSTe	29
Mulligan, Deirdre, staff counsel, Center for Democracy and Technology	40
Pincus, Andrew J., General Counsel, United States Department of Commerce	7
Reidenberg, Joel R., professor of law, Fordham University School of Law	50
Szafran, Marc, general counsel, Entertainment Software Ratings Board, Privacy Online	33
Zuck, Jonathan, president, Association for Competitive Technology	44

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Berman, Hon. Howard, a Representative in Congress from the State of California: Prepared statement	4
Bernstein, Joan Z., Director, Bureau of Consumer Protection, Federal Trade Commission: Prepared statement	16
Bruening, Paula J., director of compliance and policy, TRUSTe: Prepared statement	30
Goodlatte, Hon. Bob, a Representative in Congress from the State of Virginia: Prepared statements	56
Mulligan, Deirdre, staff counsel, Center for Democracy and Technology: Prepared statement	42
Pincus, Andrew J., General Counsel, United States Department of Commerce: Prepared statement	8
Reidenberg, Joel R., professor of law, Fordham University School of Law: Prepared statement	51
Szafran, Marc, general counsel, Entertainment Software Ratings Board, Privacy Online: Prepared statement	35
Zuck, Jonathan, president, Association for Competitive Technology: Prepared statement	46

APPENDIX

Material submitted for the record	67
---	----

PRIVACY AND ELECTRONIC COMMUNICATIONS

THURSDAY, MAY 18, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS AND
INTELLECTUAL PROPERTY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to call, at 10 a.m., in Room 2237, Rayburn House Office Building, Hon. Howard Coble [chairman of the subcommittee] presiding.

Present: Representatives Howard Coble, James F. Sensenbrenner Jr., Bob Goodlatte, Edward A. Pease, Mary Bono, Howard L. Berman and Rick Boucher.

Staff present: Blaine Merritt, Chief Counsel; Chris Katopis, Counsel; Eunice Goldring, Staff Assistant; Alec French, Minority Counsel; Sampak Garg, Minority Counsel.

OPENING STATEMENT OF CHAIRMAN COBLE

Mr. COBLE. The subcommittee will come to order.

I am advised that we are competing with Clint Eastwood, and we will probably come up second best. Mr. Eastwood is on the Hill discussing the Americans with Disabilities Act. It is good that you saw fit to come with us today.

I was talking to Mr. Pincus earlier and Ms. Bernstein as well. This privacy issue, as each of you knows, visits us not only daily, but hourly, I think we need to be aware of that, and I suspect that you are aware of it.

Today the subcommittee is conducting a general oversight hearing on the subject of privacy and electronic communications. While the subcommittee explored this topic last year, Internet privacy remains timely, and I think it appropriate to revisit the issue.

They say that 1 year in the world of e-business is like 7 years in other industries. In the past year, there were numerous developments in this area that often found their way on the front page of the newspaper and on the minds of the public. These occurrences include the government's investigation of on-line advertisers, the negotiation of a "safe harbor" for data between the U.S. and the EU, the effect of a new children's privacy law, and several class action lawsuits again leading on-line companies.

Today we will hear from an array of witnesses who represent the three elements of the privacy equation, self-regulation, technology and government regulation. Each element broaches a range of relevant questions for the subcommittee, including the role of intellec-

tual property in the development of new privacy methods, as well as the available court remedies for users in the multijurisdictional world of the Internet.

I now turn to the Ranking Member Mr. Berman for an opening statement.

Mr. BERMAN. Thank you very much, Mr. Chairman.

I usually don't make opening statements, but on this issue I would like to, and I have an even longer opening statement which I would like to submit for the record.

Mr. COBLE. Without objection, so ordered.

Mr. BERMAN. I personally share the concerns of many Americans about the information practices of some Web sites and on-line companies. I also believe these information practices raise serious policy issues, many of which are directly under this subcommittee's jurisdiction.

It appears nearly everyone, from consumer advocates to Internet marketers, agrees that consumer concerns about Internet privacy must be addressed. Unfortunately, the agreement appears to end there. The diversity of players on this issue is matched by a diversity of suggested solutions.

I am therefore pleased you have gathered a broad range of witnesses who advocate everything from wide-ranging legislation, to industry self-regulation, to user empowerment technologies. I hope we can have a freewheeling discussion, where witnesses respond to one another's proposals.

To set the table, I note that all of these approaches—legislation, self-regulation, and technology—appear to have up sides and down sides.

By the time legislation dealing with the Internet has wended its way through the legislative and regulatory processes, further evolutions in the Internet revolution may have made it obsolete. Furthermore, legislation is, by its nature, inflexible, and thus may stifle further Internet evolutions. Lastly, the existence of a law on Internet privacy could lull consumers into a false sense of security, where they assume they no longer need to be vigilant about their privacy on-line. On the other hand, legislation and legal sanctions can greatly influence behavior, and thus provide some of the best ways to positively alter the Internet landscape.

Industry self-regulation can, by its very nature, evolve and adapt at the same speed as the market, and thus provides the greatest flexibility in addressing Internet privacy issues. Unfortunately, "can" does not mean "shall," while many major Internet players have thrown their whole-hearted support behind meaningful self-regulation, and I laud them for it, they cannot alter the behavior of bad actors who continue to employ intrusive information practices.

Finally, technology can empower consumers to protect their own privacy on-line in a customized fashion. One consumer may reconfigure her browser to prevent cookies from being placed on her hard drive, while another may decide to forego this step, and its considerable inconvenience, because he is not troubled by cookies. The problem with technological solutions is that each new solution will eventually be circumvented by a countermeasure. Further-

more, many Internet users do not have the technical skills to load and utilize these tools, and that includes me.

The evident pros and cons of all of these approaches causes me to remain open-minded about the proper way to deal with the Internet privacy issue. However, in deciding which path is correct, I will be guided by certain basic principles.

Primary among these principles is that Internet users have a right to know. They have a right to know what information a Web site or other Internet entity is collecting about them. They have a right to know what is being done with that information, and whether they can limit its collection or usage. They have a right to know whether that information is adequately protected, and to what extent they can access that information.

Secondly, any legislation in this area should narrowly address real problems. Sensational anecdotes and extensive press coverage often provide momentum for legislation—and there have been plenty of both with regard to Internet privacy issues over the past year. However, anecdotes and press are not the bases for sound policy-making. Internet privacy legislation, in particular, should respond to an empirically demonstrated need because Congress must be careful not to stifle the explosive growth and creativity of the Internet medium.

Third, policy should not discriminate unnecessarily between the virtual and physical worlds. Legislation that burdens Internet businesses more than physical businesses disadvantages those Internet businesses. Conversely, legislation that burdens Internet business less than physical businesses unfairly disadvantages those physical businesses. Such inequities should only be created where necessitated by overriding policy concerns.

These principles aside, there are a variety of issues relating to Internet privacy that I hope the witnesses will address.

I understand that the privacy seal programs register their seals as certification or service marks. I am interested to learn when seal programs would revoke the right of a seal recipient to use their certification mark, and their plans for enforcing their rights against Web sites that may post this seal without authorization. I would be interested to hear opinions about whether marks for privacy seals should be considered abandoned if, one, a seal recipient is allowed to continue using the seal despite repeated noncompliance with the program; or, two, a seal program does not bring suit against every Web site that uses the seal without authorization. I am interested in the extent to which this debate about Internet information practices is really about privacy, marketing or security. Do the information practices on Web sites violate a Web surfer's right of privacy, threaten his security, or merely bombard him with annoying marketing?

Related to this is the issue of whether different classes of information and classes of consumers deserve different levels of protection. The argument that a U.S. citizen should have a right to keep private information regarding her health conditions or financial records is stronger than the argument that a U.S. citizen has a right to prevent collection of anonymous information regarding his click stream. Likewise, it is sound public policy to require that Web sites receive parental consent prior to collecting personally identi-

able information from children. However, it seems a bit patronizing and unreasonable to claim a privacy violation when an adult consumer voluntarily signs up for free Internet access that is provided on condition she allow tracking of her click stream.

Finally, I would like to thank all the witnesses in advance for taking the time to testify today and to commend them for devoting their skill and energy to tackling this difficult issue. Though your approaches and proposals may vary significantly, all of your efforts on this issue will make a positive contribution to its resolution.

Mr. COBLE. I thank you, Mr. Berman.

[The prepared statement of Mr. Berman follows:]

PREPARED STATEMENT OF HON. HOWARD BERMAN, A REPRESENTATIVE IN CONGRESS
FROM THE STATE OF CALIFORNIA

Mr. Chairman, thank you for putting together this hearing on Internet privacy issues. I share the concerns expressed by large percentages of U.S. consumers regarding the information collection and usage practices of Web sites and online companies. I believe, as is suggested by several surveys, that these concerns must be adequately addressed for the Internet to reach its full social and commercial potential. Further, I believe these information collection and usage practices raise serious policy considerations, many of which are directly under this Subcommittee's jurisdiction.

It appears that there is widespread agreement among consumer advocates, Internet industry groups, legislators, the Administration, and the international community that consumer concerns about Internet privacy must be addressed. Unfortunately, the agreement appears to end there. The diversity of players on this issue is matched by a diversity of suggested solutions.

Therefore, I am particularly interested to listen to our witnesses today, whose views I understand run the gamut of suggested solutions: from wide-ranging legislation, to industry self-regulation, to user empowerment through technological solutions. I hope we can have a relatively free-wheeling discussion, where witnesses are afforded the opportunity to respond to the approaches proposed by one another.

In looking at this issue, it appears to me that the commonly suggested solutions, legislation, self-regulation, and technology, each have upsides and down sides.

By the time legislation dealing with the Internet has wended its way through the legislative and regulatory processes, it may have been made obsolete by further evolutions in the Internet revolution. Furthermore, legislation is, by its nature, inflexible, and thus may stifle further Internet evolutions. Lastly, the existence of a law on Internet privacy could lull consumers into a false sense of security, where they assume they no longer need to be vigilant about their privacy online. On the other hand, legislation and legal sanctions can greatly influence behavior, and thus provide some of the best ways to positively alter the Internet landscape.

Industry self-regulation can, by its very nature, evolve and adapt at the same speed as the market, and thus provides the greatest flexibility in addressing Internet privacy issues. Unfortunately, "can" does not mean "shall." While many major Internet players have thrown their whole-hearted support behind meaningful self-regulation—and I laud them for it—they cannot alter the behavior of "bad actors" who continue to employ intrusive information collection and usage practices.

Finally, technology can empower consumers to protect their own privacy online, and allows consumer to protect their privacy to the exact degree that they desire. In other words, a consumer troubled by the intrusive aspects of cookies can reconfigure her browser to seek her consent whenever a Web site attempts to place cookies on her hard drive. Another consumer can decide to forgo this step, and its considerable attendant inconvenience, because he is not troubled by cookies. The problem with technological solutions is that technology development is a leapfrogging process, where each new solution is sure to be circumvented eventually by a countermeasure. Furthermore, many Internet users do not have the technical skills to load and utilize these technical tools.

The evident pros and cons of all these approaches causes me to remain open-minded about the proper way to deal with the Internet privacy issue. Thus, I am ready to be persuaded that any or all of these approaches are proper. However, in deciding which path is correct, I will be guided by certain basic principles.

Primary among these principles is that *Internet users have a right to know*. They have a right to know what information a web site or other Internet entity is collect-

ing about them. They have a right to know what is being done with that information, and whether they can limit its collection or usage. They have a right to know whether that information is adequately protected, and to what extent they can access that information. Stating that consumers have a right to know of course begs the question: what is the best method for protecting and preserving this right to know?

Secondly, *any legislation in this area should narrowly address real problems.* Sensational anecdotes and heavy press attention often provide momentum for legislation, and there have been plenty of both with regard to Internet privacy issues over the past year. However, anecdotes and press are not the bases for sound policy-making, and Internet privacy legislation in particular should respond to an empirically demonstrated need. I say "in particular" because I am particularly cautious about legislating in the Internet context, where Congress must be careful not to stifle the explosive growth and creativity of the Internet medium.

Third, *policy should not discriminate between the virtual and physical worlds.* Legislation that places burdens on Internet businesses not borne by physical businesses disadvantages those Internet businesses. Conversely, legislation that places a lower burden on Internet business than physical businesses unfairly disadvantages those physical businesses. Such inequities should only be created where necessitated by overriding policy concerns.

These principles aside, there are a variety of issues relating to Internet privacy that fascinate me, and I hope the witnesses will be able to address them either in testimony or in response to further questions.

I understand that the privacy seal programs register their seals as certification or service marks—varieties of marks protected under the Lanham Act. The status of privacy seals as certification or service marks provides seal programs with a potential array of mechanisms to ensure that licensees comply with their program requirement. Furthermore, the status of seals as marks provides seal programs with mechanisms to prevent a "bad actor" from falsely posting this seal on their Web site. I hope to find out from the seal programs the circumstances under which they would revoke from a Web site the right to use their certification mark, and their plans for enforcing their rights against the innumerable Web sites that may post this seal without authorization.

While registration of a mark provides certain rights, it also creates certain obligations for the mark holder. For example, a mark for a privacy seal may be considered abandoned if the seal program doesn't take action to prevent a program participant from using it after repeated non-compliance with the program. Abandonment may also occur if the seal provider does not bring suit against those who use it without authorization. Therefore, I would be interested to hear from other witnesses the circumstances under which they believe marks for seals should be considered abandoned.

Though I doubt we will have time to fully discuss it today, I am interested in the extent to which this debate is about "privacy", marketing, or security. As a matter of constitutional law, a U.S. citizen does not appear to have a "privacy" right against other private entities collecting their personal information or tracking their Internet meanderings. However, it is clear that Congress has the authority to pass legislation creating such a right for citizens. The question then becomes what such a new right would protect: a citizen's privacy, sense of security, or freedom from annoying marketing? Obviously, there are strong public policy imperatives to protect a citizen's reasonable expectation of privacy, but less strong policy imperatives to protect consumers against annoying commercial solicitations.

Related to this is the issue of whether different classes of information and classes of consumers deserve different levels of protection. The argument that a U.S. citizen should have a right to keep private information regarding her health conditions or financial records is stronger than the argument that a U.S. citizen has a right to prevent collection of anonymous information regarding his "click stream." Likewise, it is sound public policy to require that Web sites receive parental consent prior to collecting personally identifiable information from children. However, it seems a bit patronizing and unreasonable to claim a privacy violation when an adult consumer voluntarily signs up for free Internet access that is provided on condition she allow tracking of her "click stream."

The international elements of this issue also merit discussion, and I understand that our first panel will touch on these. The Internet is a truly international medium; a Web surfer may go from a U.S.-based Web site to an Australian site with a single click, and without knowing the national location of either site. In this environment, how can Internet privacy legislation be effective? If Congress were to outlaw certain information collection and usage practices, would those companies simply move outside U.S. borders and continue their practices?

In a related vein, I am interested to hear the Department of Commerce describe the Safe Harbor Principles it recently negotiated with the European Union in order to provide certain U.S. companies with protection against interruption of data flows under the EU Data Protection Directive. These negotiations presented one of the first contexts in which the U.S. and a foreign government tried to hammer out an understanding regarding the extent to which conflicting legal regimes that cover the Internet can be imposed on one another's citizens. I hope the Department of Commerce will be able to share with us its thoughts and insights into lessons learned from these negotiations.

As you are all aware, several dozen bills have been introduced this Congress that touch on this Internet privacy issue. Before looking at new legislation, it is always wise to look for lessons that may be drawn from prior legislation in related areas. Thus, I am particularly interested to hear from the FTC what lessons or observations it can impart to us as a result of its efforts to implement the Child Online Privacy Protection Act.

Finally, I would like to thank all the witnesses in advance for taking the time to testify today, and to commend them for devoting their skill and energy to tackling this difficult issue. Though your approaches and proposals may vary significantly, all of your efforts on this issue will make a positive contribution to its resolution.

Mr. COBLE. Our first witness today is no stranger to this subcommittee. Andrew Pincus serves as the general counsel and is the chief legal advisor for the Department of Commerce. Beyond his legal responsibilities, Mr. Pincus also serves as a senior policy advisor for the Secretary and the Department on a broad range of domestic and international issues, including electronic commerce, international trade, telecommunication, intellectual property rights, environmental issues, export controls and technology. Mr. Pincus holds a bachelor of arts degree from Yale College in 1977, where he graduated cum laude, and a law degree from the Columbia University School of Law in 1981, where he was the James Kent Scholar, Harlan Fiske Stone Scholar and notes and comments editor of the Law Review.

Joan Z., or Jodie, Bernstein is the Director of the Federal Trade Commission's Bureau of Consumer Protection. She was appointed to that post in 1995 by FTC Chairman Pitofsky. In her current post, Director Bernstein's priorities include identifying fraud, deception and the unfair practices that cause the greatest consumer harm, both on-line and off-line alike. She has headed various enforcement actions and headed several projects targeted at privacy on the Internet.

In addition, Ms. Bernstein served as general counsel of the U.S. Environmental Protection Agency, general counsel of the Department of Health and Human Services, the assistant to the Director and Acting Director of the Bureau of Consumer Protection, as well as working in private practice. She is a native of Galesburg, Illinois, and received her bachelor of arts degree in economics from the University of Wisconsin and her law degree from Yale School.

The subcommittee has copies of the witnesses' testimony, which, without objection, shall be made part of the record.

Folks, pardon my extended introduction because only we on the subcommittee know these witnesses. Many of you perhaps don't, and I think it is important for you to know their backgrounds.

I am pleased to indicate that we are joined by the gentleman from Virginia Mr. Boucher, the gentlelady from California Ms. Bono, and the gentleman from Indiana Mr. Pease.

I am told that there will be votes on or about 10:45, so that will disrupt us for a while.

Mr. Pincus, you may remember we go with a 5-minute rule here. All witnesses are asked to confine their oral testimony to 5 minutes. Now, when you see that red light illuminate in your eyes, that does not mean that Mr. Berman and I are going to take you behind the barn and shoot you. It does mean that it is time to wrap it up because we are on a fairly short leash today. We have your written statements, and I say that for the benefit of the second panel as well. Try to comply with the 5-minute rule.

Mr. Pincus, welcome back to the subcommittee. We are glad to have you with us.

**STATEMENT OF ANDREW J. PINCUS, GENERAL COUNSEL,
UNITED STATES DEPARTMENT OF COMMERCE**

Mr. PINCUS. Thank you. It is an honor to be here to discuss this important issue; also to be here with Ms. Bernstein, who, when I was a lawyer returning to the private practice, took a risk on me as her lawyer, and we have known each other ever since.

Privacy has long been a fundamental value for Americans, and along with the great promise of the information age, wider dissemination of information and the tremendous engine that it is providing for our economy, and the ability of individuals to use technology to protect their privacy, comes the risk that privacy might be diminished. That is a matter of concern because of the high value that we place on an individual's ability to protect their privacy, but also it is a threat to the future of this medium because it is clear if consumers don't have confidence that the Internet is a safe place to shop or to work or to play, they won't do that, and this medium won't realize its potential. Poll after poll and every other indicator of consumers' views indicates that privacy is an issue in consumer confidence with respect to the Internet.

Since the President and the Vice President issued their Framework for Global Electronic Commerce in July 1997 and identified privacy as a concern that had to be addressed if the Internet was to realize its potential, and directed Secretary Daley to work with the Federal Trade Commission to address that issue, it is something that the administration has been very focused on.

The fundamental principles of privacy are supplied by fair information practices which have been memorialized by the OECD as the touchstone of what good privacy practices are for the private sector. The most fundamental of these, while they are all important, is notice to the consumer what is going to be done with your information, the choice about whether that is okay, and some kind of enforcement mechanism to make sure that those notice and choices are honored.

What is clear about privacy is that there is no one-size-fits-all approach. Especially with the different business models that are developing in this dynamic economy, there are very different privacy concerns, and they really do warrant different solutions. With respect to especially sensitive information, the administration has concluded legislation appropriate, and we have supported the legislation that was passed by Congress and has been implemented by the FTC with regard to children's privacy. The Department of Health and Human Services has proposed regulations with respect to health privacy, and with respect to financial information, a first

step in the Gramm-Leach-Bliley bill, and the President last month sent to the Hill a proposal to address some additional issues with respect to that issue, and we hope that is something taken up by Congress.

With respect to on-line privacy or on-line information generally, we have challenged the private sector to create effective self-regulatory mechanisms. Why? For reasons that you all mentioned in your opening statements. This is a fast-moving medium, new issues arise, and it will be difficult for the legislative processes to grapple with, because as the law is passed, there is a risk that problem will become past, and new ones will arise. And this medium is global, and in anything dealing with the Internet, we have to try to fashion solutions that will work on a global basis, and self-regulation, if it is effective, can do that because unlike government rules, self-regulatory mechanisms don't have to be. And also by creating—for new enforcement mechanisms in the private sector, government can become the enforcement of last resort, and self-regulation can provide real remedies rather than the illusion of a remedy that might not be available because of a lack of resources or interest by whoever is supposed to do the enforcing.

This process was slow in getting started, and Secretary Daley talked individually to the business community and made a number of speeches prodding the process. We have seal programs, BBBOnLine and TRUSTe, for example. The key question is will those models become ubiquitous in the private sector. There is a problem of the free riders and bad actors, but we have to recognize the distinction between those two issues. We don't—in addressing how do we get everyone into a good program, we don't want to undercut the fact that the self-regulatory models out there provide tremendous benefits.

Another reason self-regulation is appropriate is that these are not static issues. Self-regulatory mechanisms can be updated to deal with them or new ones created. One example is the workshop that we held with the FTC on on-line advertising, which indicated a new problem, profiling, and a new group has come forward to try to develop a self-regulatory system to address that.

In response to questions I will talk about the EU safe harbor because my red light is on.

[The prepared statement of Mr. Pincus follows:]

PREPARED STATEMENT OF ANDREW J. PINCUS, GENERAL COUNSEL, UNITED STATES
DEPARTMENT OF COMMERCE

Thank you for the opportunity to testify here today. The rapid growth in the use of the Internet, for both personal and commercial purposes, has led to increased public concern about personal privacy. In fact, privacy is one of the most important concerns of Internet users. The promise of information technologies—their ability to facilitate the collection, re-use and instantaneous transmission of information—can, if not managed carefully, pose risks to personal privacy. This Administration has worked hard to protect the privacy of personal information that is communicated online and is proud of its record. During my testimony, I will summarize some of the Administration's efforts in this area. I will also mention a number of private sector initiatives that are designed to address privacy concerns.

A Framework for Global Electronic Commerce, issued by the Administration on July 1, 1997, recognizes that it is essential to assure personal privacy in the networked environment if people are to feel comfortable doing business online. In the Framework, President Clinton and Vice President Gore set forth three privacy priorities for their administration: encouraging private sector development and

adoption of effective codes of conduct, rules and technological solutions to protect privacy on the Internet; developing recommendations on the appropriate role of government in privacy protection; and ensuring that means are developed to protect the privacy of children.

With regard to children's, financial, and medical information—the highly sensitive categories of information—this Administration has supported technologically neutral legislative solutions to protect privacy online. In other areas, we have worked with the business community, privacy advocates, and academics to create effective self-regulatory regimes. We have also acted with the knowledge that the Federal Trade Commission ("FTC") has enforcement powers that allow it to protect consumers from unfair and deceptive trade practices that affect privacy interests. In addition, there are a number of statutory or regulatory regimes that apply to an equal degree both online and off-line. The Fair Credit Reporting Act is an example of one such regime.

Fair information practices form the basis for the Privacy Act of 1974, the legislation that protects personal information collected and maintained by the United States government. In 1980, these principles were adopted by the international community in the Organization for Economic Cooperation and Development's Guidelines for the Protection of Personal Data and Transborder Data Flows. Principles of fair information practices include awareness, choice, appropriate levels of security, data integrity, consumer access to their personally identifiable data, and accountability.

In 1997, the President directed the DOC and the Office of Management and Budget ("OMB") to work with the private sector to develop and implement effective, consumer-friendly, self-regulatory privacy regimes. In response to that directive, the DOC has engaged in significant consultations with industry, members of the academic community, public interest groups and the international community to consider what characteristics of a self-regulatory program would be necessary to protect privacy effectively. Throughout these consultations, we have pointed to the principles of Fair Information Practices as a necessary basis of private sector self-regulation. In addition to the Fair Information Practices that I will describe below, a self-regulatory privacy regime should include mechanisms to ensure compliance with the rules and appropriate recourse to an injured party when rules are not followed. When companies make assertions that they are abiding by certain privacy practices and then fail to do so, they may be liable for deceptive practices and subject to action by the FTC or other appropriate regulatory authorities.

Awareness, a first fair information principle, requires notice to the consumer of the identity of the collector of their personal information, the intended uses of the information, and the means by which they may limit its disclosure. Companies are responsible for raising consumer awareness and can do so through privacy policies that articulate the manner in which a company collects, uses, and protects data, and the choices they offer consumers with regard to their personal information. Companies should display their privacy policies prominently, so that they are available before consumers are asked to provide personal information to the company. Privacy policies must be written in clear and easily understood language. Finally, consumer education that teaches individuals to ask for relevant knowledge about why personal information is being collected, what the information will be used for, how it will be protected, the consequences of providing or withholding information, and any recourse they may have, helps consumers to understand privacy policies.

Choice, a second fair information principle, requires that consumers are given the opportunity to exercise choice with respect to whether and how their personal information is used, either by businesses with whom they have direct contact or by third parties. Consumers must be provided with simple, readily visible, available, and affordable mechanisms—whether through technological means or otherwise—to exercise this option. For certain kinds of information, e.g., medical and financial information or information related to children, more rigorous mechanisms for choice are sometimes appropriate. A number of factors determine the type of choice that is appropriate in a particular setting. For example, the Administration has taken the view in proposed medical privacy rules that individuals must affirmatively consent (i.e. opt-in choice) to the disclosure of their health records for non-health related purposes.

A third fair information principle, security, holds that companies creating, maintaining, using or disseminating records of identifiable personal information must take reasonable measures to assure its reliability for its intended use and must take reasonable precautions to protect it from loss, misuse, alteration or destruction. Companies should also strive to assure that the level of protection extended by third parties to whom they transfer personal information is at a level comparable to their own.

A fourth principle, data integrity, requires that companies keep only personal data relevant for the purposes for which it has been gathered, consistent with the principles of awareness and choice. To the extent necessary for those purposes, the data should be accurate, complete, and current.

A fifth fair information principle, access, means that consumers should have the opportunity for reasonable, appropriate access to information about them that a company holds, and be able to correct or amend that information when necessary. The extent of access may vary from industry to industry depending on the nature of the information collected, the number of locations in which it is stored, the nature of the enterprise, and the ways in which the information is to be used.

A sixth principle, accountability, holds companies accountable for complying with their privacy policies. A self-regulatory privacy regime should include mechanisms to ensure compliance with the rules and appropriate recourse to an injured party when rules are not followed. Such mechanisms are essential tools to enable consumers to exercise their privacy rights, and should, therefore, be readily available and affordable to consumers. Companies that collect and use personally identifiable information should offer consumers mechanisms by which their complaints and disputes can be resolved. Such mechanisms should be readily available and affordable. One such mechanism is verification to attest that the assertions businesses make about their privacy practices are true and that privacy practices have been implemented as represented. The nature and the extent of verification depends upon the kind of information with which a company deals—companies using highly sensitive information may be held to a higher standard of verification. The failure to comply with fair information practices should have consequences. Ultimately, sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion. When companies make assertions that they are abiding by certain privacy practices and then fail to do so, they may be liable for deceptive practices and subject to action by the FTC or other appropriate regulatory authorities.

Based on these principles, I would like to describe some of the specific actions we have taken to protect the privacy of American consumers. I will also address some of the initiatives that the private sector has pursued to enhance privacy protections online.

ONLINE PRIVACY: ADMINISTRATION INITIATIVES ON SELF-REGULATION AND INDUSTRY IMPROVEMENT

In June of 1998, the FTC reported to Congress on the state of privacy practices online. The FTC found that the practices of Web sites demonstrated a real need for implementing basic fair information practices. The FTC report encouraged industry progress in addressing consumer concerns regarding online privacy through self-regulation. It pointed to effective self-regulation as a desirable means to protect privacy online because it allows firms to respond quickly to technological changes and employ new technologies to protect consumer privacy. The report did conclude, however, that an effective self-regulatory system had yet to emerge. Finally, the FTC recommended that Congress develop legislation placing parents in control of the online collection and use of personal information from their children. As I will discuss later, that legislation is in place, with the full support of this Administration.

Also in June of 1998, the DOC requested comments from the public on various aspects of Internet privacy, including the effectiveness of self regulation for privacy. It also asked for responses to specific questions concerning online privacy protection and input on the specific instances in which government action may be necessary to protect privacy on the Internet. A review of these comments has aided the DOC in its initiatives to improve the handling of consumers' private information.

In that same month, Secretary Daley opened the DOC's two-day online privacy summit by challenging the private sector to implement enforceable privacy protections to ensure that consumers can feel confident that their personal information is safe online. The Secretary called on industry to move swiftly to enact a self-regulatory regime to protect privacy in business transactions on the Internet and warned that without meaningful progress, the government may have to explore regulatory solutions.

There has been significant progress in private sector self-regulation since the FTC's June 1998 report and the DOC's privacy summit. The DOC conducted extensive outreach to the business community, privacy advocates, and academics to address the privacy concerns. An important example of private sector progress to calls for increased privacy protections was the creation of third-party seal organizations that certify a web site's compliance with its privacy policy. More than 2,000 web sites belong to these organizations, nearly double the number that participated last

year. BBBOnline and TRUSTe are among the most prominent. According to TRUSTe, they currently have 1,582 licensees, with almost 1,000 applicants in various stages of the approval process. The percentage of small to medium sized businesses participating in this seal program is encouraging. Overall, 85 percent of TRUSTe's licensees report annual gross revenue of \$10 million or less. Furthermore, more businesses are applying for TRUSTe seals. This year, TRUSTe reports that 150 to 200 companies apply for their seal per month, up from 100 to 150 companies last year. The private sector has also displayed awareness of the need to comply with TRUSTe's seal requirements as their business models change. Of TRUSTe's current licensees, one-third have asked TRUSTe for a new approval after changing their online privacy practices. BBBOnline has 482 licensees and 1,028 applicants. Approximately 60 new companies apply for the BBBOnline privacy seal every month.

The creation of the Online Privacy Alliance ("OPA") in June of 1998 represents another meaningful response by industry to the need to strengthen privacy protections online. The OPA brings together more than 80 of the largest companies doing business on the Internet and 23 business organizations that represent thousands of other companies in an alliance to promote privacy online. The OPA participated in the DOC's Privacy Summit and enacted guidelines implementing the fair information practices described in the Framework involving notice, choice, access, and security. The OPA developed its cross-sector guidelines to accommodate a broad range of industry sectors that include marketers, individual reference services companies, brick and mortar establishments and even small Web startups. All these industry sectors can use the OPA guidelines to establish privacy practices and post privacy policies that best suit their business models and customer expectations.

For instance, after the formation of the OPA, BBBOnline and TRUSTe modified their own licensee requirements to be consistent with the OPA. Other seal programs have incorporated the OPA Guidelines to meet the needs of their respective industry sectors. The Entertainment Software Rating Board (ESRB) has established a seal for software-related industries and CPA's WebTrust program leverages the CPA brand to instill confidence in its seal program. Further, new technologies such as the Platform for Privacy Preferences ("P3P") and palm-sized Internet interfaces can easily be incorporated into this self-regulatory model.

The May 1999 release of the Georgetown Internet Privacy Policy Survey and the ("OPA") Top 100 survey demonstrated that the private sector initiatives that I have just described represent significant improvement in online self-regulation in one year. The Georgetown Survey looked at 364 ".com" Web sites, a random sampling selected from the 7,500 most visited Web sites. The Georgetown Survey found 65.7 percent had posted at least one type of privacy disclosure (privacy policy notice or an information practice statement). The OPA survey showed that 94 percent of the top 100 Web sites had posted at least one type of privacy disclosure, up from 71 percent from last year.

In March of 1999, IBM announced that it would strengthen consumer privacy online by choosing to restrict its advertising to sites that post privacy policies. Secretary of Commerce William H. Daley then wrote letters to top web advertisers, urging them to follow IBM's lead. In the last year, companies including Microsoft, Disney, Intel, Compaq, Novell, American Express, and Proctor and Gamble have heeded the Secretary's call and implemented advertising policies that mirror IBM's. These market leaders, which account for more than one-third of America's top 20 web advertisers, use their resources to bring real privacy protection to Internet users by creating incentives for more web sites to provide privacy protection.

NetCoalition.com, a group of leaders in the information technology industry, is campaigning to educate web users on privacy issues—teaching them how they can protect their privacy. Recently, NetCoalition.com sent a letter from ten of the information technology industry's top executives to 400 Internet companies asking them to develop comprehensive privacy policies, inform Web users about their information collection practices, give consumers access to the information that companies have collected, and allow users some control of how such information is used.

In July of 1999, the FTC released "Self-Regulation and Privacy Online: A Report to Congress." The 1999 report presented the results of FTC's examination of developments in the growth of the Internet as a commercial marketplace and in consumers' and industry's responses to the privacy issues posed by the online collection of personal information. The FTC noted that significant progress industry had made significant progress in providing consumers with notice of their practices and concluded that legislation to regulate online privacy was not necessary. The report cited the Georgetown Internet Privacy Policy survey and the OPA Top 100 survey as evidence of private sector progress. OPA guidelines and the seal programs as evidence of industry leaders' substantial effort and commitment to fair information practices.

The 1999 report also concludes, however, that only a small minority of commercial web sites have joined these programs and that implementation of fair information practices is not widespread among commercial Web sites. The FTC found that the challenge for industry was to educate those companies which do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation.

In July of 1998, Vice President Gore had also called on the DOC to work with the FTC to encourage companies that build profiles about individuals to implement effective self-regulatory mechanisms. The FTC's 1999 report also recommended that the DOC and the FTC held a profiling workshop in November of 1999. This workshop focused on "online profiling," the practice of aggregating information about consumers' preferences and interests, gathered primarily by tracking their movements online, and using the resulting consumer profiles to create targeted advertising on Web sites. Profiling typically employs "cookies," text files placed on users' computers to store information about their computers and their online activities.

At this workshop, Secretary Daley called for industry leadership in protecting consumer privacy in online profiling. During the workshop, the companies in this industry announced the formation of a new self-regulatory group, the Network Advertising Initiative ("NAI"). The NAI committed to develop a web site to provide consumers an opportunity to opt out from the services of these companies. The group also is working on a set of principles to provide effective privacy protection in the area of profiling. Also, as a result of the workshop and the NAI announcement, the Direct Marketing Association ("DMA") added a new component to its privacy policy generator that requires members of the DMA to announce on their sites whether they are using a third-party profiler. The DOC and the FTC also sought public comment addressing various issues related to the practice of online profiling. The comment period closed on November 30, 1999.

Another initiative that the 1999 FTC report called for was the creation of a task force charged with defining the parameters of the principles of consumer access to data and adequate security. This task force is the Advisory Committee on Online Access and Security ("ACOAS"). ACOAS has provided advice and recommendations to the Commission regarding implementation of certain fair information practices by domestic commercial Web sites. Public comments for consideration by ACOAS were due by April 28, 2000. In particular, ACOAS addressed providing online consumers reasonable access to personal information collected from and about them and maintaining adequate security for that information.

INTERNATIONAL USE OF SELF-REGULATORY MODEL:

Turning briefly to the importance of the self-regulatory model to the U.S. in the international arena, the safe harbor arrangement that the DOC and the European Commission have tentatively reached clearly demonstrates that self-regulation is seen as an effective means of protecting personal privacy. When the European Directive on Data Protection became effective in 1998, it was not clear how this "adequacy" requirement would apply to the U.S., since the U.S. does not have omnibus privacy legislation like the EU.

Given the billions of dollars in transatlantic trade in services, both the U.S. and the EU recognized the Directive presented a very serious issue. In response, the DOC, working with the European Commission, developed the concept of "safe harbor" to bridge the gap between our different approaches to data protection. In essence, the safe harbor is a self-regulatory framework that provides "adequate" protection for data from Europe. Enforcement of the commitment to abide by the safe harbor rules is assured in several ways, including through self-regulatory seal programs and similar mechanisms. It is also backed by the authority of the FTC and other government agencies to take action against unfair and deceptive trade practices. As Secretary Daley indicated recently, the safe harbor "demonstrates that both the EU and the U.S. recognize that a carefully constructed and well-implemented system of self-regulation, as advocated by the President and the Vice President, can protect privacy rights." Both sides are now in the process of consulting with their respective domestic authorities and constituencies on this "safe harbor" arrangement.

The DOC consulted extensively with the Congress, the private sector, consumer groups and others during the course of the safe harbor discussions. This consultation occurred in many briefings and meetings on the issue, as well as more informally through other exchanges. Indeed, it would not have been possible to conduct the discussions without the thoughtful advice and consultation from the Congress, the private sector, consumer groups, and the American public.

TECHNICAL SOLUTIONS TO PROTECT PRIVACY ONLINE:

The Administration has also worked with the private sector to develop technical solutions to protect privacy online. The Internet technical community has completed work on the specifications for a number of technologies to empower consumers to protect privacy online. These technologies allow consumers to determine their privacy preferences and have them automatically communicated to web site operators. It will take additional time to bring applications based on these specifications to the market, but they will assist individuals, companies, and self-regulatory organizations in the protection of privacy.

For example, the Platform for Privacy Preferences ("P3P") will enable Web sites to express their privacy practices to users in a standard format that can be retrieved and interpreted automatically. P3P will allow users to be informed of site practices (in both machine—and human—readable formats) and to automate decision-making based on these practices when appropriate. In essence, P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personal information. Another example of private sector technical innovation designed to protect online privacy is Microsoft's Kids Passport service. Kids Passport is a turnkey solution that will be available to Web sites for managing parental consent and helping sites comply with the Children's Online Privacy Protection Act ("COPPA").

PRIVACY IN THE FEDERAL GOVERNMENT:

The *Framework* also focused on addressing the appropriate role of government in privacy protection. In March of 1999, the President created the position of Chief Counselor for Privacy to coordinate the federal government agencies' wide range of efforts related to privacy issues. The Chief Counselor for Privacy serves in OMB's Office of Information and Regulatory Affairs, which oversees implementation of the Privacy Act of 1974. This office handles a wide range of privacy-related issues from the public and private sectors.

For example, OMB oversees federal agencies' implementation of the Privacy Act of 1974, 5 U.S.C. Section 552a (1988) protects individuals from most non-consensual government disclosure of private information. In May 1998, President Clinton issued a Memorandum for Heads of Executive Departments and Agencies directing all agency heads to take specific action to assure that the use of new information technologies sustain privacy protections provided by applicable statutes and that information is handled in full compliance with the Privacy Act.

In June of 1999, the OMB directed all federal agencies to post privacy policies on government web sites by September 1, 1999. As of September 1, 1999, 100 percent of all federal agencies have posted privacy policies. By December 1, 1999, federal web sites went a step further and posted these policies at points of entry to the web site and other areas where substantial personal information is collected.

ADMINISTRATION SUPPORT FOR PRIVACY LEGISLATION COVERING SENSITIVE INFORMATION:

The *Framework* also called on the Administration to ensure that means are developed to protect the privacy of children. Since 1997, the Administration has acted to protect information relating to children and other sensitive information dealing with medical and financial records. We have also supported legislation to prevent the on-line theft of personal information. In these areas, the Administration recognized that self-regulation was not an appropriate mechanism to safeguard the privacy interests at stake. We chose to pursue legislative solutions because, in these sensitive areas, a stronger response was required.

October 30, 1998, the President signed into law, the "Identity Theft and Assumption Deterrence Act of 1998." This legislation makes identity theft a federal crime, with penalties generally of up to three years imprisonment and a maximum fine of \$250,000. Specifically, the legislation penalizes the unlawful use or transfer of personal information with the intent to commit an unlawful act, such as obtaining fraudulent loans or credit cards, drug trafficking, or other illegal purposes. It also directs the FTC to help victims deal with the consequences of this crime.

Looking to the protection of children's information, the President supported and signed COPPA. COPPA ensures that sites aimed at children under the age of 13 must obtain verifiable parental consent before they gather and use personal information received from the children. In the fall of 1999, the FTC issued the final regulations implementing COPPA. The rules went into effect on April 21, 2000. Under the rules, sites must get parental permission via mail, fax, credit card, or digital signature before disclosing a child's personal information to a third party. If a site

plans to use the information internally, the company can rely on consent via e-mail from a parent, at least for the first two years. After that, the FTC will require sites to get more "reliable" parental consent (fax, mail, credit card) for all information collected. In addition, the new rules also require children's sites to post privacy notices and give parents the option of prohibiting the sale of information that has been collected for internal use.

Congress discussed financial privacy intensively in the course of its financial modernization debate last year. As the President pointed out when signing the law, the modernization law took significant steps to protect the privacy of financial transactions, but did not go far enough. The President asked OMB, the Department of Treasury, and the National Economic Council to craft a legislative proposal to close loopholes under existing law. On April 30, he announced his plan to protect consumers' financial privacy. This plan would include:

1. *Consumer choice*: Giving consumers the right to choose whether a firm can share consumer financial information with third parties or affiliated firms.
2. *Enhanced protection for especially sensitive information*: Requiring that a consumer give affirmative consent before a firm can gain access to medical information within the financial conglomerate, or share detailed information about a consumer's personal spending habits.
3. *Access and correction*: Giving consumers a new right to review their information and correct material errors.
4. *Effective enforcement*: Providing effective enforcement tools for financial institutions subject to Federal Trade Commission enforcement of privacy rules.
5. *Comparison shop on privacy policies*: Giving consumers privacy notices upon application or request so they know how information is protected before a customer relationship is established.

These provisions were introduced in the House as H.R. 4380, attracting immediate and substantial support in both the House and the Senate. As Secretary of the Treasury Lawrence Summers emphasized on March 7, "It's time to start now."

There has been a longstanding appreciation in the United States that individual medical records include especially sensitive information. Disclosing medical data can reveal what is happening inside a person's body, such as a report that a person is HIV positive, or inside a person's mind, such as the transcript of a session with a psychotherapist. The Federal government has recognized these concerns at least since 1973, when the Department of Health, Education, and Welfare first announced the basic fair information practices that underlie privacy policy today.

Congress recognized the need for legal protection of medical records when it passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA). After extensive discussions with stakeholders and as required by HIPAA, the Secretary of Health and Human Services issued her recommendations for health privacy legislation in September 1997. Congress was unable to meet the HIPAA deadline for enacting comprehensive privacy legislation by August 21, 1999. Accordingly, the President and Secretary Shalala announced proposed privacy regulations on October 29 of last year. It was HHS's goal to make the regulation process open to those who wanted to communicate their concerns in person. HHS met with many individuals and organizations to hear their concerns and clarify provisions of the proposed rule. HHS received over 53,000 submissions of comments by the February 17, 2000 deadline. HHS is now considering those comments, and the regulations will become final this year.

Although the medical privacy regulations will become final this year, there is a pressing need for further Congressional action. As HHS Assistant Secretary Margaret Hamburg testified in February of this year: "Health information privacy is a top priority for the Department and the Administration, and we continue to believe that legislation is the only way to achieve the goal." President Clinton explained some of the reasons for legislation when he proposed the privacy regulations last October. The Administration is especially concerned that the enforcement powers under current law are not as effective as they should be. We recommend federal legislation that would allow punishment of those who misuse personal health information and redress for people who are harmed by its misuse. Administration officials have testified often on what should be included in medical privacy legislation, and we urge that there be no delay on this subject.

CONCLUSION:

In conclusion, I would like to underscore this Administration's long-standing belief that for the Internet to meet its full potential, the American public must feel that

their consumer rights and privacy are protected online. Where legislative solutions were appropriate, we acted swiftly to support the enactment of responsible legislation.

In the three years since President Clinton challenged the private sector to make self-regulation a reality with respect to online privacy, we have worked with industry, privacy advocates, and academics and have made significant progress. The seal programs that have been developed provide effective privacy protection. We are concerned, however, that while many leaders in the private sector have demonstrated their commitment to effective self-regulation, industry as a whole needs to do much more to achieve the goal of making this approach ubiquitous in the online environment.

Thank you again for the opportunity to appear before you.

Mr. COBLE. Ms. Bernstein.

STATEMENT OF JOAN Z. BERNSTEIN, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Ms. BERNSTEIN. Thank you, Mr. Chairman. I am very happy to be with you here today and particularly appreciate the opportunity that you have given the Commission to report to you on the Commission's initiatives on on-line privacy. As you noted, Mr. Chairman, in your remarks, with the remarkable growth in e-commerce has come increased consumer awareness and also concern about the on-line collection and use of personal data. Indeed surveys have shown that a high percent of the consumers, 92 percent, are concerned about the misuse of their personal information on-line. With respect to children's privacy, the concern consumers have expressed is even greater.

The Commission has been involved in addressing on-line privacy issues for some time. It is a 5-year history which began in 1995. In a general way the Commission has done the following. We have held a series of public workshops on the subject, we have conducted two extensive surveys of commercial Web site information practices, and we have issued two reports to Congress on the subject.

A third report will be issued soon on the second survey of U.S. commercial Web sites that were conducted in February and March of this year.

Obviously from this background the Commission goal has been to understand the new marketplace and its information practices and to try to assess the cost and benefits to business and consumers. The Commission has encouraged self-regulation and has worked very closely with the private sector to do that. At the same time, the Commission has also used our law enforcement authority under section 5 of the FTC Act to stop unfair deceptive information practices by on-line companies as we have with off-line companies.

Two years ago the Commission recommended to Congress that it enact legislation to protect children's on-line privacy. Our recommendation was based on the 1998 survey of children's Web sites, which showed that while a vast majority of sites were collecting personal information from kids, few had privacy policies. Only 1 percent of sites sought parental permission to collect information from children. Within 4 months of our recommendation, the Congress enacted, as you know, the Children's On-Line Privacy Protection Act of 1998, sometimes called COPPA.

COPPA, or, as I call it, the Kids Act, is the first Federal legislation specifically to address on-line privacy. It was enacted with the support of a broad constituency of industry privacy advocacy and consumers groups and requires four basic things for kids under the

age of 13. It provides parents with notice of the information practices. It requires Web sites to obtain verifiable parental consent before collecting personal information from kids. It provides parents with access to the information collected from their children, and it requires that the information be maintained in a secure and confidential manner.

Last month the Commission's rule implementing the act became effective. We had worked closely with on-line businesses, self-regulatory groups, States, advocates to craft a rule that would be both effective and enforceable, yet flexible enough to accommodate rapid innovation.

In education we have taken a very aggressive role in attempting to carry out what we think is a critical role, and that is to educate business consumers and so forth on what the requirements of the new rule are. We, for example, issued a compliance guide that posted—that was posted on the FTC Web site. We also issued a consumer alert that was strictly for parents, and at the same time the FTC developed a kids' privacy Web site where information about the act and the rule was placed.

We brought along a couple of posters today to demonstrate part of the education campaign. The kids' privacy is the home page on the Web site. It has proven to be very successful. Many parents have written and called us to tell us how effective the Web site has been. There have been as many as 50,000 visits to that Web site.

To ensure even broader corporate participation in the awareness campaign, the Commission is publishing a notice in the Federal Register with details on participation. We have had an enormous number of companies that have participated with us in order to get the message out to all parents and consumers generally.

We also believe that law enforcement will be critical to the act's success. We expect to receive complaints as we have in the past and will follow up on those complaints to bring law enforcement actions as appropriate.

We will continue to work with our education efforts and our enforcement efforts. We look forward to working with the subcommittee to address these issues, and I will be pleased to answer questions.

Mr. COBLE. Thank you, Ms. Bernstein.

[The prepared statement of Ms. Bernstein follows:]

PREPARED STATEMENT OF JOAN Z. BERNSTEIN, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. Chairman and Members of the Subcommittee, I am Jodie Bernstein, Director of the Bureau of Consumer Protection of the Federal Trade Commission. I appreciate this opportunity to report on the Commission's recent initiatives in online privacy, and, in particular, the history and implementation of the Children's Online Privacy Protection Act.¹

I. INTRODUCTION AND BACKGROUND

A. FTC Law Enforcement Authority

The FTC's mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and to increase consumer choice by promoting vigorous competition. As you know, the Commission's re-

¹ My oral testimony and any responses to questions reflect my own views and are not necessarily the views of the Commission or any other Commissioner

sponsibilities are far-reaching. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTCA"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.² With the exception of certain industries and activities, the FTCA provides the Commission with broad investigative and law enforcement authority over entities engaged in or whose business affects commerce.³ Commerce on the Internet falls within the scope of this statutory mandate.

B. Privacy Concerns in the Online Marketplace

Since its inception in the mid-1990's, the online marketplace has grown at an exponential rate. Recent figures suggest that as many as 90 million Americans now use the Internet on a regular basis.⁴ Of these, 69%, or over 60 million people, shopped online in the third quarter of 1999.⁵ In addition, the Census Bureau estimates that retail e-commerce reached \$5.3 billion for the fourth quarter of 1999.⁶

With this remarkable growth in e-commerce has come increased consumer awareness that online businesses are collecting and using personal data, and increased consumer concern about the privacy of this data. Recent survey results demonstrate that 92% of consumers are concerned (67% are "very concerned") about the misuse of their personal information online.⁷ The level of consumer unease is also indicated by a recent study in which 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential.⁸ The Commission's online privacy efforts have been directed in large measure toward engaging the private sector in addressing these concerns, to ensure the continued growth of the online marketplace.

C. The Commission's Approach to Online Privacy—Initiatives since 1995

Since 1995, the Commission has been at the forefront of the public debate on online privacy. The Commission has held public workshops; examined Web site information practices and disclosures regarding the collection, use, and transfer of personal information; and commented on self-regulatory efforts and technological devel-

² 15 U.S.C. § 45(a).

³ The Commission also has responsibility under 45 additional statutes governing specific industries and practices. These include, for example, the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms, and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 30 rules governing specific industries and practices, e.g., the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices; and the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312. The Commission has also issued a final rule implementing the Gramm-Leach-Bliley Act, 115 U.S.C. §§ 6801 *et seq.*, which is discussed below.

The Commission does not, however, have criminal law enforcement authority. Further, under the FTCA, certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance, are wholly or partially exempt from Commission jurisdiction. See Section 5(a)(2) and 6(a) of the FTC Act, 15 U.S.C. § 45(a)(2) and 46(a). See also the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

⁴ The Intelliquist Technology Panel, *Panel News*, available at <<http://www.techpanel.com/news/index.asp>> (hereinafter "Technology Panel") (90 million adult online users as of third-quarter 1999). Other sources place the number in the 70-75 million user range. See Cyber Dialogue, *Internet Users*, available at <<http://www.cyberdialogue.com/resource/data/ic/index.html>> (69 million users); Cyberstats, *Internet Access and Usage, Percent of Adults 18+*, available at <<http://www.mediamark.com/cfdocs/MRI/cs-199a.cfm>> (75 million users).

⁵ Technology Panel. This represents an increase of over 15 million online shoppers in one year. See *id.*

⁶ United States Department of Commerce News, *Retail E-commerce Sales for the Fourth Quarter 1999 Reach \$5.3 Billion, Census Bureau Reports* (Mar. 2, 2000), available at <<http://www.census.gov/mrts/www/current.html>>.

⁷ Alan F. Westin, *Personalized Marketing and Privacy on the Net: What Consumers Want, PRIVACY AND AMERICAN BUSINESS* (Nov. 1999) at 11. See also IBM Multi-National Consumer Privacy Survey, prepared by Louis Harris & Associates Inc. (Oct. 1999), at 72 (72% of Internet users very concerned and 20% somewhat concerned about threats to personal privacy when using the Internet); Forrester, *Online Consumers Fearful of Privacy Violations* (Oct. 1999), available at <<http://www.forrester.com/ER/Press/Release/0,1769,177,FF.html>> (two-thirds of American and Canadian online shoppers feel insecure about exchanging personal information over the Internet).

⁸ Survey Shows Few Trust Promises on Online Privacy, Apr. 17, 2000, available at <<http://www.nyt.com>> (citing recent Odyssey survey).

opments intended to enhance consumer privacy.⁹ The Commission's goal has been to understand this new marketplace and its information practices, and to assess the costs and benefits to businesses and consumers.

In June 1998 the Commission issued *Privacy Online: A Report to Congress* ("1998 Report"), an examination of the information practices of commercial sites on the World Wide Web and of industry's efforts to implement self-regulatory programs to protect consumers' online privacy.¹⁰ Based in part on its extensive survey of over 1400 commercial Web sites, the Commission concluded that effective self-regulation had not yet taken hold.¹¹ The Commission recommended that Congress adopt legislation setting forth standards for the online collection of personal information from children; and indeed, just four months after the 1998 Report was issued, Congress enacted the Children's Online Privacy Protection Act of 1998 ("COPPA"), which authorized the Commission to issue regulations implementing the Act's privacy protections for children under the age of 13.¹² COPPA and the Commission's Rule implementing the Act are discussed in greater detail below.

In the 1998 Report, the Commission deferred its recommendations with respect to the collection of personal information from online consumers generally. In subsequent Congressional testimony, the Commission discussed promising self-regulatory efforts suggesting that industry should be given more time to address online privacy issues. The Commission urged the online industry to expand these efforts by adopting effective, widespread self-regulation based upon the long-standing fair information practice principles of Notice, Choice, Access, and Security, and by putting enforcement mechanisms in place to assure adherence to these principles.¹³ In its 1999 report to Congress, *Self-Regulation and Privacy Online*, the Commission again recommended that self-regulation be given more time, but called for further industry

⁹ The Commission held its first public workshop on privacy in April 1995. In a series of hearings held in October and November 1995, the Commission examined the implications of globalization and technological innovation for competition and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices regarding the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. The Commission held a second workshop in June 1997 to explore issues raised by individual reference services, as well as issues relating to unsolicited commercial e-mail, online privacy generally, and children's online privacy.

The Commission and its staff have also issued reports describing various privacy concerns in the electronic marketplace. See, e.g., *FTC Staff Report: The FTC's First Five Years Protecting Consumers Online* (Dec. 1999); *Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 1997); *FTC Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996); *FTC Staff Report: Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996). Recently, at the request of the Department of Health and Human Services ("HHS"), the Commission submitted comments on HHS' proposed Standards for Privacy of Individually Identifiable Health Information (required by the Health Insurance Portability and Accountability Act of 1996). The Commission strongly supported HHS' proposed "individual authorization" or "opt-in" approach to health providers' ancillary use of personally identifiable health information for purposes other than those for which the information was collected. The Commission also offered HHS suggestions it may wish to consider to improve disclosure requirements in two proposed forms that would be required by the regulations. The Commission's comments are available at <<http://www.ftc.gov/be/v000001.htm>>.

¹⁰ The Report is available on the Commission's Web site at <http://www.ftc.gov/reports/privacy3/index.htm>.

¹¹ 1998 Report at 41.

¹² 15 U.S.C. §§ 6501 et seq.

¹³ The Commission has supplemented its own fact-finding by soliciting public input on pressing issues to the implementation of fair information practices online. In December 1999, the Commission convened an Advisory Committee on Online Access and security, a group comprising 40 e-commerce experts, industry representatives, security specialists, and consumer and privacy advocates, to advise the Commission on the options for implementing the fair information practice principles of Access and Security online. The Advisory Committee proceedings are available at <<http://www.ftc.gov/acoas>>.

In November, 1999, the Commission, together with the Department of Commerce, held a public workshop on "online profiling," the practice of aggregating information about consumers' interest, gathered primarily by tracking their movements online, and using the resulting consumer profiles to deliver targeted advertisements on Web sites. The Commission will soon report to Congress about concerns raised by online profiling, as well as industry's self-regulatory efforts in this area. The transcript of the Workshop, as well as public comments filed in connection with the Workshop, are available at <<http://www.ftc.gov/bcp/profiling/index.htm>>.

efforts to implement the fair information practice principles and promised continued Commission monitoring of these efforts.¹⁴

In February and March of this year, the Commission conducted its second survey of U.S. commercial Web sites. The survey assessed websites' compliance with fair information practices by analyzing the nature and substance of their stated policies regarding the collection, use and disclosure of personal information gathered from consumers online. The Commission will report to Congress in the near future on the results of its 2000 survey.¹⁵

Last week, the Commission issued a final Rule implementing the privacy provisions of the Gramm-Leach-Bliley Act.¹⁶ The Rule requires a wide range of financial institutions to provide notice to their customers about their privacy policies and practices. The Rule also describes the conditions under which those financial institutions may disclose personal financial information about consumers to nonaffiliated third parties, and provides a method by which consumers can prevent financial institutions from sharing their personal financial information with nonaffiliated third parties by opting out of that disclosure, subject to certain exceptions.

D. Law Enforcement Actions

The Commission has also brought several law enforcement actions, pursuant to its mandate under the FTCA, to remedy online companies' unfair and deceptive practices with respect to the collection and use of consumers' personal information. In February, 1999, the Commission settled charges that GeoCities, one of the most visited websites, had misrepresented the purposes for which it was collecting personal identifying information from both children and adults.¹⁷ In the Liberty Financial case, the Commission challenged allegedly false representations by the operator of a "Young Investors" site that information collected from children in an online survey would be maintained anonymously.¹⁸ Most recently, in the ReverseAuction.com case, the Commission settled charges that this online auction site had obtained consumers' personal identifying information from a competitor's site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business.¹⁹ These cases demonstrate the Commission's ongoing commitment to protecting consumers' online privacy as an integral part of its law enforcement mission.²⁰

III. PROTECTING CHILDREN'S ONLINE PRIVACY

A. Public Concerns about Children's Online Privacy

Children are among the fastest growing populations on the Internet. The number of children online has almost tripled in just the last two years, growing from nearly

¹⁴ *Self-Regulation and Privacy Online* (July 1999) at 12-14 (available at <<http://www.ftc.gov/os/1999/9907/index.htm#13>>).

¹⁵ The Commission has supplemented its own fact-finding by soliciting public input on pressing issues related to the implementation of fair information practices online. In December 1999, the Commission convened an Advisory Committee on Online Access and Security, a group comprising 40 e-commerce experts, industry representatives, security specialists, and consumer and privacy advocates, to advise the Commission on options for implementing the fair information practice principles of Access and Security online. The Advisory Committee's Report, which was presented to the Commission earlier this week, will be discussed in the Commission's upcoming report to Congress on online privacy. The Advisory Committee proceedings are available at <<http://www.ftc.gov/acsoas>>.

In November, 1999, the Commission, together with the Department of Commerce, held a public workshop on "online profiling," the practice of aggregating information about consumers' interests, gathered primarily by tracking their movements online, and using the resulting consumer profiles to deliver targeted advertisements on Web sites. The Commission will soon report to Congress about concerns raised by online profiling, as well as industry's self-regulatory efforts in this area. The transcript of the Workshop, as well as public comments filed in connection with the Workshop, are available at <<http://www.ftc.gov/bcp/profiling/index.htm>>.

¹⁶ 16 C.F.R. Part 313; available at <<http://www.ftc.gov/opa/2000/05/glbpress1.htm>>.

¹⁷ GeoCities, FTC Dkt. No. C-3849 (Feb. 12, 1999) (consent order).

¹⁸ Liberty Financial, FTC Dkt. No. C-3891 (Aug. 12, 1999) (consent order).

¹⁹ FTC v. ReverseAuction.com, Inc., No. 00-0032 (D.D.C. Jan. 6, 2000) (consent decree).

²⁰ Since the fall of 1994, the Federal Trade Commission has brought over 125 law enforcement actions against over 360 companies and individuals to halt fraud and deception on the Internet. The FTC has not only attacked traditional schemes that have moved online, like pyramid and credit repair schemes, but also has brought suit against pagejacking, mouse trapping, modem hijacking, fraudulent e-mail marketing, and other hi-tech schemes that take unique advantage of the Internet. The Commission pioneered the "Surf Day" concept, and has searched the Net with over 250 law enforcement or consumer groups worldwide, targeting specific problems and warning consumers and new entrepreneurs about what the law requires. The Commission has also posted "teaser pages" online, i.e., fake scam sites that educate consumers to enable them to avoid Internet ruses.

10 million in 1997²¹ to almost 26 million by the end of 1999.²² That number will continue to rise as the Internet becomes an increasingly integral part of American culture, education, and commerce.

Online marketers have responded to this growth with sites targeting children and offering a diverse array of products, services and other features. Like sites targeted to older consumers, these sites often collect personally identifying information from young consumers. Our 1998 survey found that of the 212 children's websites surveyed, 89% were collecting personal information from children, including names, home addresses, e-mail addresses, and in one case, information about family finances.²³ However, only 24% of those sites posted privacy policies, and only 1% of those sites sought parental permission to collect such information.²⁴ These practices were in sharp contrast to parents' beliefs about what information should be collected from their children. A 1997 Louis Harris/Allan Westin survey found that 72% of parents objected to the collection of names and addresses from their children, even if that information was used only within the company, and 97% of parents objected if the information was to be released to third parties.²⁵

B. Children's Online Privacy Protection Act (COPPA)

Reacting to these concerns, in October 1998 Congress enacted the Children's Online Privacy Protection Act, the first federal legislation specifically to address online privacy. The statute was enacted with the support of a broad coalition of industry, privacy advocates and consumer groups, and drew heavily on the experience of industry self-regulatory groups in attempting to establish workable guidelines for the protection of children's privacy online.

The legislation requires operators of commercial websites directed to children under 13 to:²⁶

- provide parents with notice of their information practices;
- obtain verifiable parental consent before collecting most personal information from children;
- provide parents with access to the information collected from their children;
- limit data collection to that which is reasonably necessary to participate in the activities offered at the site; and
- maintain the security and confidentiality of the information they collect.

COPPA required that the Commission issue rules implementing these requirements within one year of its enactment. Like the legislative consideration of COPPA, our rulemaking process, too, drew on the accumulated expertise of online businesses, self-regulatory groups, State Attorneys General, and privacy and children's advocates. We received over 145 comments and held a widely attended workshop to gather information to help us craft a rule that would be both effective and enforceable, yet flexible enough to accommodate the rapid technological innovation that characterizes this ever-changing medium. As required by COPPA, we issued the final Rule in October 1999, and it became effective last month.

COPPA and its implementing rule contain several important features. First and foremost, both the Act and the Rule employ flexible performance standards rather than static rules. This not only provides website operators with flexibility in choosing how to comply, but also leaves room for the growth of new technologies. For example, COPPA's definition of the key concept of "verifiable parental consent" encompasses "any reasonable effort, taking into account available technology," to ensure that a parent receives the required notice and consents to the operator's collection of information. This flexible standard will encourage the development of new products and services that can help make compliance with the Rule easy and inexpensive.²⁷ In fact, the Commission has committed to undertake a review in eighteen

²¹ Cyber Dialogue, "Children on the Internet," InterActive Consumers (May 1997).

²² Cyber Dialogue, "Online Children," InterActive Consumers (Dec. 1999).

²³ 1998 Report at 31-33.

²⁴ Id. at 35-37.

²⁵ Louis Harris & Associates and Dr. Alan F. Westin, Commerce, Communication, and Privacy Online, A National Survey of Computer Users (1997).

²⁶ COPPA also covers operators of commercial sites who knowingly collect information from children under 13. 15 U.S.C. § 6502(a)(1).

²⁷ The Commission is aware of recent press reports of websites that have chosen to discontinue services to children under 13 because of perceived difficulties in complying with the Rule. See "Parents Remain Unclear on Online Privacy Law," Cybertimes, New York Times (May 12, 2000). The Commission will monitor these reports as it considers future actions under the Rule.

months to determine whether new and developing technologies are available for use in obtaining "verifiable parental consent" under the Rule.

Another feature of the Act and Rule is a "safe harbor" provision, designed to encourage continued self-regulatory efforts to protect online privacy. Over the years, self-regulatory groups have developed substantial expertise in monitoring, detecting, and addressing online privacy problems. Website operators have long consulted with the self-regulatory groups on the privacy issues they face. Under COPPA, self-regulatory programs can now apply to have their programs accepted as "safe harbors" from Commission or State Attorney General enforcement.²⁸ Several proposals are currently under review by the Commission.

C. Implementing the COPPA Rule

Now that the Rule is in effect, the Commission is attempting to address two key issues: business and consumer education and enforcement.

1. EDUCATION

The Commission has used a variety of creative, novel and cost effective ways to educate parents, children and website operators about the provisions of the COPPA. As it has in all its education efforts, the Commission has made extensive use of the Internet to disseminate its messages.²⁹ In November, shortly after the final Rule was announced, a Compliance Guide was posted on the FTC website.³⁰ E-mails were sent to major children's sites, participants in COPPA workshops, and commentators in the rulemaking to alert them to the guidance. In addition, the Commission is holding informal seminars to educate online businesses about the need to comply with COPPA.

In addition to the FTC's own website, the Commission hosts and maintains www.consumer.gov, a one-stop shop for consumer information from the federal government. The site, which was initiated by the FTC in 1996 with a small group of other agencies, now links to information from over 160 federal agencies and has more than 80,000 unique visits a month. It has housed an array of special education initiatives, involving Y2K, health care quality, consumer fraud, and identity theft, a 21st century crime involving the misappropriation of personally identifying information. The original www.consumer.gov team received the Hammer Award from the National Performance Review.

In February, the FTC issued a Consumer Alert geared to parents, introducing them to the new law. The Alert was sent to more than 14,000 news media, as well as to websites, parent organizations and schools through organizations like the PTA and the National Association of Elementary School Principals. The media mailing alone resulted in more than 100 interviews with Commission staff about the provisions of the Rule. Articles appeared in hundreds of newspapers, including the print and web editions of *USA Today*, the *Wall Street Journal* and the *New York Times*, and on radio and television networks and stations. Media exposure no doubt contributed to the fact that the Consumer Alert was accessed more than 32,000 times on the FTC's website in April alone.

At the same time, the FTC developed a Kidz Privacy website where information about COPPA was placed. Major national corporations and privacy advocacy groups joined in our outreach efforts.³¹ Among the participants: AOL, Center for Democracy

²⁸ In addition to the FTC, COPPA confers authority on the States to bring actions in Federal District Court to enforce compliance with the FTC's implementing rule. 15 U.S.C. 6504.

²⁹ The FTC has dramatically extended the reach of its educational messages by making available more than 200 consumer and business publications on its website, www.ftc.gov. Last year, views of these publications numbered 2.5 million (up from 140,000 in 1996).

³⁰ An important part of the FTC's education mission is to provide guidance to web businesses. Many of these entrepreneurs are small, start-up companies that are new to the Internet and to marketing in general, and are unfamiliar with consumer protection laws. The Commission has several special publications that are especially well-designed to give practical, plain English guidance to this audience (e.g., *Advertising and Marketing on the Internet: Rules of the Road; Dot Com Disclosures*). The agency also has used other approaches to provide guidance to those who are engaged in e-commerce, e.g., posting compliance guides and staff advisory letters on the Web, using the trade press to promote the availability of information, and holding public workshops on online issues.

³¹ The FTC often partners with private sector members to disseminate educational messages. For example, the FTC has actively recruited partners to link to its website and to place public service banner announcements provided by the FTC on their sites. Links from the public service banners allow visitors to click through to the FTC site quickly to get the information they're looking for exactly when they want it. Among the varied organizations that have helped drive traffic to the valuable information on www.ftc.gov are AARP, American Express, the Arthritis

and Technology, Center for Media Education, Chancery Software, CyberAngels, Disney/Go.com Network, Headbone.com, Lycos, Microsoft, NetFamilyNews, NetNanny Software, Surfmonkey.com, and Wiredkids. All these sites link to the FTC site. In addition, Chancery Software designed and printed 40,000 bookcovers and bookmarks with children's online privacy tips to distribute to school children. To ensure that all organizations interested in protecting children's privacy online have the opportunity to participate in the COPPA Public Awareness Campaign, the Commission is publishing a notice in the Federal Register with details on how to participate.

In addition to sections for kids, adults, business and the media, the Kidz Privacy website also includes radio public service announcements and a banner public service announcement that can be downloaded and placed on any website. The banner would enable viewers at any site on the web to click directly to the Kidz Privacy site. In May and September, radio public service announcements will air which refer listeners to the FTC website and the Commission's Consumer Response Center for more information.

The Consumer Response Center provides education and assistance to individual consumers and businesses who contact us by calling our toll free helplines (877-FTC-HELP and 877-ID-THEFT), by writing us, or by using our online complaint form at www.ftc.gov. CRC counselors provide information, assist consumers in resolving their complaints where possible, and enter complaints into the Commission's extensive complaint database which is used for law enforcement.³² The CRC is now responding to some 40,000 contacts a month, covering a broad spectrum of inquiries and complaints.³³ With the implementation of COPPA and growing consumer awareness and concern about privacy, we may begin to receive more inquiries and complaints in this area.

2. Rule Enforcement

We have been impressed by the substantial commitment the online industry has made to implementation of the statute and their commitment to the fair information practices principles that underlay it. Nonetheless we believe that along with education, enforcement will play a critical role in the Act's success. Initially, we expect to receive referrals from industry self-regulatory groups, privacy advocates, competitors, and consumer groups. We also will analyze complaints collected by the CRC to identify rule violations. In addition, the Commission intends, as it has done on many occasions, to hold "surf" days in which FTC staff work together with other enforcement agencies to identify sites that are not in compliance with the law. The Commission also is holding joint training sessions with our State law enforcement partners, to help facilitate active and coordinated enforcement of the Rule.

For the most part, website operators have been working diligently to comply with the Rule. In some instances the benefits go beyond the online environment. For example, one offline magazine which also operates a website has revised its policies on publishing the full names and ages of children making submissions to its magazine, and now posts those submissions using only the child's first name and age.

III. CONCLUSION

The Commission will continue its efforts, in close cooperation with its private sector partners, to expand its consumer and business education campaigns, and to assure broad compliance with the law. We look forward to working with the Subcommittee to address these online privacy issues and are pleased to answer any questions you may have.

Mr. COBLE. Ms. Bernstein, can you explain what happens when a Web site deceptively misappropriates the trademark, logo or brand of a seal provider? Let me ask you this. Does it occur often, does the Bureau have a role in that situation when it occurs, and what remedies are available to both consumers and the affected

Foundation, the Better Business Bureau, CBS, CNN, Circuit City, the National Institutes of Health, the U.S. Patent and Trademark Office, and Yahoo.

³² Fraud complaints also are entered into the Consumer Sentinel database which is maintained by the FTC and now contains more than 250,000 consumer fraud complaints. More than 100 organizations contribute complaints to the Consumer Sentinel database, which is shared with over 240 law enforcement agencies in the U.S. and Canada. Consumer Sentinel makes the data available through a secure website and also provides a variety of tools to help law enforcers investigate and prosecute fraud.

³³ Contacts range from complaints about get-rich-quick telemarketing scams and online auction fraud, to questions about consumer rights under various credit statutes, to requests for educational materials.

parties, A? And B, is current trademark law adequate to protect consumers who rely on seal providers in those deceptive cases?

Ms. BERNSTEIN. Let me try to answer, and if necessary we will follow up with more detailed answers following the hearing. We do not have—excuse me, my voice seems to be going.

Andy, do you want to answer?

Mr. COBLE. Do you want to weigh in on that, Mr. Pincus?

Mr. PINCUS. I think on the trademark side, to the extent those seals have been registered as marks and are being used without authorization on a site, I would think that those mark holders would have trademark remedies against the people who are using their marks without authorization.

Ms. BERNSTEIN. The Commission does, of course, have its section 5 authority, which, if there were deceptive practices involved in the misuse of a trademark, of course the Commission has authority to do that.

We do not have extensive information at the present time that they are being deceptively used, but we would certainly be happy to work with the committee and with our own staff in order to be sure that that occurs. Of course, I think you are referring to the fact that the seal programs, of course, also have authority under the Lanham Act to take actions of their own to police that marketplace. And TRUSTe has reported to us that they have developed a software program to monitor the use or misuse of the seals and take action against those that are being used deceptively.

Mr. COBLE. I thank you.

Mr. Pincus, you have explained that the safe harbor package is an example of the success of the United States and the EU systems coming together. What is on the horizon as United States companies wish to compete in other parts of the world? Is the Internet Corporation for Assigned Names and Numbers, that is the ICANN model, appropriate for settling privacy disputes that arise from different legal jurisdictions?

Mr. PINCUS. Mr. Chairman, I think that perhaps some analog to ICANN is appropriate. We hope that the EU safe harbor, which we hope will be concluded at the end of this month, except for financial services, as to which there will be continuing discussions, and the maintenance of the standstill agreement that is now in effect generally. Our view is that it is a good example of the Europeans recognizing that you don't need a law in order to protect privacy because their approach is very different. They have an across-the-board law that applies to everything. At the beginning of the process, I think there was a question about whether they would view self-regulation as a viable alternative, and the good thing both for privacy and generally for other issues that may arise with respect to the Internet, like consumer protection, is that they have recognized that it can be just as good; we think better, of course, but at least they have said just as good.

I think the seal programs themselves could provide that to the extent they begin to become international, and I know that some of them are looking hard at that possibility, and analogs are being developed in other countries, maybe seals backed up by private sector processes that can be used in the same way that the ICANN is being used under the domain name space to address these issues

without having consumers rely on the very unlikely fact that they might get access to court in some faraway place to vindicate their rights.

Mr. COBLE. The recent news reports describe a wave of privacy litigation, including class actions coming out of State courts. How do you see the relationship of the legal system of the States on the one hand and the Federal Government on the other shaping Internet privacy for consumers and the growth of the Internet. If the Congress chooses more regulation, should State preemption be considered in some areas? I see my red light is illuminated. But I put the question before it came on, so would you please respond?

Mr. PINCUS. I am not familiar with the details of the lawsuits. I think generally we have taken the view that State laws, to the extent that they apply provide good backup, especially if they are being used, just from press reports, to address claims of unfair deceptive practices in terms of companies saying that they are doing one thing and not doing another.

I think historically, we have relied on a two-tier system to provide an effective network of remedies, and I think that would continue to be the case here. And generally we have seen the States as a supplement to whatever exists on the Federal level.

Ms. BERNSTEIN. And we at the Commission have worked effectively with the States in various consumer protection areas. For example, in the telemarketing area where the Congress set a national standard for telemarketing practices, it also authorized the State attorneys general to enforce the standard, but it was a uniform standard, in Federal court. It has worked extremely well because it really put 51 cops on the beat, at the same time providing a business, I think, with a national standard that they could comply with. So in a sense it is a model that could be used in the privacy area as well. In fact, to some extent we expect to do that with the children's rule working with the States.

I think the important thing is is there a national standard. The enforcement can be separately managed if the Federal Government and the State governments are working together. It has been our experience that it has been a good working relationship.

Mr. COBLE. I thank you both.

I am pleased now to recognize the gentleman from California Mr. Berman.

Mr. BERMAN. Thank you, Mr. Chairman.

Mr. Pincus, press reports indicate that the FTC might as early as next week come out in favor of legislation, privacy legislation, dealing with the collection and use of personal information for adult Web surfers.

In your testimony you differentiated between the need for legislation in certain areas, financial, health, children's information, and support for self-regulation in general. Can I assume that at this point the administration, at least in your eyes, does not want to suggest a proposal that would eliminate the time for the industry to demonstrate that self-regulation can adequately protect the less sensitive personal information of adult Web surfers?

Mr. PINCUS. Yes, Congressman Berman. Of course, we haven't seen the FTC surf results or their recommendation.

I think for us there are two—as I tried to lay out, there are two separate issues in on-line. One is what is the model that you are going to use, and we think that the private sector has come up with a good model in these seal programs.

And then there is the sort of next question, which is, okay, if you have a good model out there, how do we be sure that it becomes ubiquitous? What do you with the bad actors and the free riders to get them under the tent?

What we have said, and what Secretary Daley said on a number of occasions in the last several months, is that we are concerned that the progress in getting people into good privacy programs and seal programs has not been moving as quickly as we would like, although there has been progress measured maybe in non-Internet time, and Internet time is quicker, and the challenge will be if consumers don't feel that enough progress is being made and they don't feel safe.

So the question is when is the time to do that, and the quite complicated question is even if one decides it is the right time, how do you create a mechanism that provides the benefits, keeps the benefits of self-regulation and the seal programs, which we think are tremendous, but provides either carrots or sticks or both to get them to become ubiquitous. And we think designing that, even if one makes the leap to say that legislation is necessary, will be a difficult task, but one that will be essential in order to not throw the baby out with the bath water as it were.

Mr. BERMAN. What does the FTC think of that answer?

Ms. BERNSTEIN. Mr. Pincus's answer?

Mr. BERMAN. Yes. Or the administration's position? If you are going to do it next week, you may not want to speak about it this week.

Ms. BERNSTEIN. Unfortunately, I can't.

Mr. BERMAN. All right, let me withdraw the question.

Mr. Pincus, an appealing aspect of a legislative approach is to make every Web site disclose their privacy policies and what data they are collecting, and what they are doing with it, and how they are keeping it secure. I gather, though, that when you look at those Web sites which post a privacy policy, many of them are practically incomprehensible to the average person. If we were to legislate it, it is hard to legislate making things understandable as well as informative or complete. I am curious what you think would happen and what FTC's experience is with COPPA. To what extent are these Web site disclosures useful to people?

Mr. PINCUS. I agree it is hard to legislate, although one can have standards. With self-regulatory, there is an institution out there policing them that doesn't take government resources, that is self-supporting.

A bigger problem with that than just the disclosure approach is that, in our view, that is not enough to meet good privacy policy. Having a privacy policy, if it says we take all of your information, and there is nothing that you can do about it, and if it is not connected to any monitoring or enforcement mechanism so if somebody has a complaint, there is no place to go, and if there is no choice given to the consumers, we think that is a problem. So our concern with that approach is that it—if that were the rule, it would be a

reduction in privacy protection compared to what the seal programs give. So we wouldn't want an approach that actually gives less privacy protection than the model that we are hoping to propagate out there in the world.

If you are a company and the law said all you have to do is disclose, your business people would say, why are we going to put all of these resources in a seal program; if Congress has said all we have to do is have disclosure, we will do that and be done with it. So we have a concern that may result in a reduction of privacy protection.

Mr. BERMAN. Thank you.

Mr. COBLE. Thank you.

We have been joined by the gentleman from Wisconsin Mr. Sensenbrenner. I think you have no questions?

Mr. SENSENBRENNER. No questions.

Mr. COBLE. The gentleman from Indiana Mr. Pease.

Mr. PEASE. Thank you, Mr. Chairman.

Thank you for your presentations. You have touched on a variety of difficult subjects. I want to ask you about one that you did not address, and I realize in a global scheme it is not as pressing as others that you have. But I have had contacts from folks in the study of genealogy and their concerns, which are I guess not atypical of folks in general in dealing with the Web. On the one hand they find it to be very helpful. On the other, they are concerned about Web sites that post information about living persons. Obviously there are some churches as tenets of their faith that study ancestry, and there are many who are interested in this subject, many because of Alex Hailey's work and others. They find that information about ancestry very helpful, but they become troubled when it starts posting information about many people still alive, many who are children.

Do either of you have any experience with that particular subject; and if so, can you share it with us?

Mr. PINCUS. I don't. It is an interesting problem that actually I haven't heard about before, and I will be happy to think about.

Ms. BERNSTEIN. And I suppose because our jurisdiction goes to commercial sites, and I think what you are describing tend to be—they are generally called chat rooms or not-for-profit, noncommercial sites, we haven't had a lot of experience.

Mr. PEASE. One point in particular seems to have appeared in concerns raised to our office, is that obviously genealogical information includes a mother's maiden name, and that is often used in industry as a password or another way of—

Ms. BERNSTEIN. It is an identifier.

Mr. PEASE. And there is a concern how that affects living persons. We will be glad to hear from you.

Mr. COBLE. We have a vote on, but I will recognize the gentleman from Virginia Mr. Boucher.

Mr. BOUCHER. Thank you, Mr. Chairman.

I read with interest over the weekend a summary of the FTC's upcoming findings, and I was very interested to note—and this was on the Web. It was on MSNBC, so it is not proprietary information. What apparently you are going to report is that in your most recent survey, your finding that 90 percent of the Web sites that col-

lect information do, in fact, post a policy that details what information they collect and how it is used. Ninety percent might sound like a high figure, but what about the other 10 percent? One might suspect that the other 10 percent will be the worst actors, that these will be the ones who compile a very comprehensive profile of commercial preferences and then assimilate that into a list along with a lot of other similar profiles and then sell that to outside parties, who then will proceed to send samples to all of the people on the list. It is that kind of practice that I think also fuels the rising public concern that we see.

I am just wondering if maybe the time hasn't come when we should have a baseline set of requirements that would apply to all Web sites, including that 10 percent that we might suspect are going to be the worst actors. Mr. Goodlatte and I have introduced a bill that would do that. It is just a baseline set of guarantees. It would say that every Web site that places cookies and collects information would have to have a posting on the site of what information is collected, how that information is used. If it is used internally, that would be indicated. If it is transmitted beyond the site, that would be indicated. And then every visitor to the Web site would have an opt-out opportunity; in other words, an opportunity to depart the Web site without any information being collected.

Now, I have heard Mr. Pincus say he is concerned if we do something like that, it might have the opposite effect from what we intend. It might discourage companies from signing up with the seal programs which contain those guarantees and perhaps some additional things, but he also mentioned that one of the problems that he sees with simply doing it this way would be perhaps a lack of enforcement. Presumably you get some kind of enforcement through a seal program, and there might not be any this way.

Ms. Bernstein, I am told that the FTC currently enforces as an unfair trade practice under section 5 of your charter legislation any failure of an organization to perform as it promises it will, so once it signs up under a seal program or some other SRO, if it doesn't publish the information that is required, if it doesn't discharge all of the obligations voluntarily undertaken, that becomes an unfair trade practice. Is that what you do today?

Ms. BERNSTEIN. Yes, it is. For a long time the Commission has had authority to do that, and going back to the National Advertising Review Board, which is a self-regulatory body, the Commission has worked as backup to enforce the self-regulatory program.

Mr. BOUCHER. If we passed a statute, we would have some enforcement authorities delineated there, perhaps conferring those on to the FTC. My concern is that I see this rising tide of public concern becoming so great that at some point the Congress is likely to respond in an even more aggressive manner and actually pass legislation that really does begin to interfere with the effective functioning of electronic commerce. That is what I would hate to see. I am concerned if something like this baseline set of guarantees doesn't go into effect reasonably soon, we are likely to see that harsher, perhaps ill-considered legislation in the category of overkill be enacted. That almost happened with regard to financial services last year, and it easily could happen with regard to information collection practices.

I guess I would ask you, Mr. Pincus, one question, and that is what do the seal programs really provide in terms of consumer protection that would not be captured within the kind of statutory approach that I have just described? In other words, what do they do beyond require publication of the information that they collect, and how it is used and provide opt-out opportunities? What beyond that do they offer?

Mr. PINCUS. They also provide their own monitoring and enforcement process. It is sort of a supplement to the Commission. It has resources.

Mr. BOUCHER. That could be done statutorily?

Mr. PINCUS. It could. Our concern is whether the resources of the Commission as the Internet grows will be adequate.

The other thing that the seal programs do is they provide the ability to opt out and—at least in some situations, and I think people on the next panel can tell you about the elements that allow you on the Web site.

Mr. BOUCHER. Thank you.

Mr. COBLE. Mrs. Bono, do you have questions?

Mrs. BONO. Yes, but with six votes, I will put my questions to the second panel.

Mr. COBLE. If need be, you can communicate with Mrs. Bernstein or Mr. Pincus at a subsequent time.

We have six votes, so you are talking 30 minutes before we all return. You all rest easily. I thank the first panel for their appearance today. We stand in brief recess.

[Recess.]

Mr. COBLE. The subcommittee will come back to order.

I am going to have to depart prior to the conclusion of the hearing, but please don't take that as lack of interest or rudeness. But I have to be at a luncheon meeting. I anticipate another vote on the floor in about an hour. I think we ought to be able to wrap it up by then and keep you all no longer than that.

This panel's first witness is Paula J. Bruening, who serves as director of compliance and policy at TRUSTe, a privacy initiative designed to stimulate the growth of electronic commerce by building consumer trust and confidence in the Internet, and shape public policy regarding Web sites' disclosure of individuals' personal and private information. Prior to TRUSTe she served positions at the NTIA, National Telecommunications and Information Administration, in the Department of Commerce, and the Congressional Office of Technology Assessment. Ms. Bruening is a graduate of John Carroll University in Cleveland, Ohio, and received her law degree at Case Western Reserve University School of Law.

Next we have Marc Szafran, who serves as general counsel of the Entertainment Software Rating Board Privacy Online Program, a nonprofit program providing specialty privacy seals focusing on entertainment. He received his law degree from the Yeshiva University Cardozo School of Law.

Our third witness is someone who is also familiar to this subcommittee. Ms. Deirdre Mulligan is a leading on-line privacy expert and consumer advocate. She is staff counsel at the Center for Democracy and Technology, where she evaluates the impact of technology on individual privacy. She is currently active in several pri-

vacy and technology initiatives. Ms. Mulligan is a graduate of Smith College and received her law degree from the Georgetown University Law Center.

Our next witness is Jonathan Zuck, president of the Association for Competitive Technology. ACT represents a range of leading high-technology computer companies that are involved in the on-line privacy debate and responsible for innovation in this area. He has studied international relations at Johns Hopkins and the School for Advanced International Studies.

Our final witness is Fordham University law professor Joel R. Reidenberg. He is a tenured member of the faculty, who specializes in information technology and privacy law, as well as a prolific author. He received his undergraduate degree from Dartmouth, his law degree from Columbia University, and holds an advanced degree from the University of Paris.

Thank you all for joining us. We have your written statements, which will be made a part of the record, and so please limit your oral testimony to 5 minutes.

Ms. Bruening, we will begin with you.

**STATEMENT OF PAULA J. BRUENING, DIRECTOR OF
COMPLIANCE AND POLICY, TRUSTe**

Ms. BRUENING. Thank you, Mr. Chairman and members of the subcommittee, for the invitation to speak today. As many of you know, TRUSTe is a nonprofit Internet privacy seal program operating independently from industry and government. For nearly 3 years we have been working to address consumer privacy concerns by awarding responsible Web businesses the TRUSTe privacy seal, a symbol that effectively communicates a site's privacy practices and provides consumers with an oversight mechanism.

Our seal program was developed by consumer and industry advocates on the premise that the most effective way to protect on-line privacy is through a standardized mechanism of informed consent coupled with effective enforcement. TRUSTe's standards are based on the core principles of fair information practices articulated by the Federal Trade Commission and the Department of Commerce as essential to an effective framework for industry self-governance. All Web sites that display the seal must give full disclosure of what information is gathered and with whom it is shared. They must provide meaningful choice, allowing consumers to prevent the sharing of that information with third parties. They are required to give reasonable access so that customers can correct any inaccuracies with their profile information; and finally, they must provide reasonable security mechanisms to protect the information that is gathered.

Web sites that display our privacy seal must subject themselves to our oversight and enforcement mechanisms, which include an increasingly recognized consumer dispute resolution mechanism called the TRUSTe Watchdog. The program is growing exponentially, both in the number of Web site participants and in the scope of our program. In July 1997, TRUSTe had a total of 15 Web site licensees. Today that number has risen to more than 1,600 with an additional 150 to 200 applications for the TRUSTe privacy seal received each month. This rapid growth has led a Web tracking com-

pany named Nielsen Net Ratings to consistently rate TRUSTe as the most prominent symbol on the Internet.

While we have done an effective job at certifying and assuring Web site privacy, we also understand that in today's increasingly networked world, data is collected at many points that are off the Web site. For that reason we plan to evolve our privacy seal program to cover more areas of the data-gathering network. Our first step will come shortly with the anticipated launch of a pilot project to address the privacy practices of software products. By evolving our program to cover more areas of the data-gathering network, we are demonstrating our ability to keep pace with technology's changes.

TRUSTe's efforts moving forward will be focused on consumer education. We fundamentally believe that Internet privacy is not just about corporate use of personally identifiable information, it is also an issue of consumer education. We are already off to a good start with consumer education with the successful execution of the Privacy Partnership. This grassroots educational campaign was launched with the support of all of the Internet portal sites and gained the participation of more than 1,600 Web sites, all donating valuable banner advertising space. Through education campaigns like the Privacy Partnership, we are working to raise awareness not only of the privacy issue, but also how consumers can best control the use of their personal information and protect themselves on-line.

I want to conclude, Mr. Chairman, by thanking you again for inviting me here today. Privacy has become a fundamental issue that can impact the healthy growth of the Internet. If we are not able to adequately address this issue, then we risk crippling the growth of the Internet and the economic benefits that flow from it. The TRUSTe program is based on the principle that consumers and citizens of the Web community have a right to control the distribution of their personal information. This right should be a right of everyone, and should be based on full disclosure and choice through a common set of business privacy practices.

To date we have been extraordinarily successful at building this framework for consumer protection, but we must realize that our work is not yet done. More Web sites must abide by these principles and subject themselves to third-party oversight. You can help our efforts by using your influence to urge companies that have not joined oversight programs to do so. Once these companies post privacy statements and join oversight programs, we can use existing laws to regulate and enforce their practices. Based on the initial success of the TRUSTe program and our future course of action, we are well on our way to creating a safer and more empowering environment on the Web.

Mr. COBLE. Thank you.

[The prepared statement of Ms. Bruening follows:]

PREPARED STATEMENT OF PAULA J. BRUENING, DIRECTOR OF COMPLIANCE AND POLICY, TRUSTe

Thank you, Mr. Chairman. My name is Paula Bruening. I am the Director of Compliance and Policy for TRUSTe. I want to start off by thanking you, Mr. Chairman, and the members of the Committee for the invitation to speak today.

As many of you know, TRUSTe is a nonprofit Internet privacy seal program operating independently from industry and government. For nearly three years, we have been working to address consumer privacy concerns by awarding responsible Web businesses the TRUSTe Privacy Seal, a symbol that effectively communicates a site's privacy practices and provides consumers with a powerful oversight mechanism. Our goal from the beginning was to establish a program easy for a consumer to understand, and to ensure compliance. With the TRUSTe seal, that is exactly what we accomplished.

Seal programs are proving to be an effective and working element for online self-governance well suited for the global and constantly changing Internet medium.

When we began development of the TRUSTe program in 1996, consumer privacy concern was barely a blip on the Internet industry's radar screen. But at the time several studies pointed to a general distrust in the medium, emanating largely from the fear that participation would compromise personal privacy. We understood that this was only the tip of the iceberg and that lack of trust would have staggering implications to the success of Internet commerce. Simply put, just as trust is critical to the healthy growth of communities, the absence of trust would cripple growth of the Internet and the economic benefits that flow from it.

However, we were confounded by a complex problem: how do you regulate business practices on a global medium that is constantly changing and fast growing? It was clear to us then that traditional mechanisms of government oversight would fail given technology's breakneck speed of change and global nature.

We developed the TRUSTe Privacy Seal program on the premise that the most effective way to protect online privacy is through a standardized mechanism of informed consent coupled with effective enforcement. In fact, the TRUSTe Privacy Seal goes beyond this model by actually engaging the Web site and the Web surfer in an open conversation about privacy practices.

I will now describe to you our program, give you an overview of how the program is doing, and tell you where TRUSTe is headed.

The foundation of the TRUSTe program is the TRUSTe Privacy Seal. In many ways, this is the online equivalent of the Good Housekeeping Seal of Approval. In fact, the TRUSTe Privacy Seal is a far more robust tool guiding appropriate industry practices and serving as a Watchdog for consumers.

Our standards are based on the core principles of Fair Information Practices, articulated by the Federal Trade Commission and the Department of Commerce as essential to an effective framework for industry self-governance. All Web sites that display the TRUSTe Privacy Seal must give full disclosure of what personal information is gathered and with whom it is shared. They must provide meaningful choice allowing consumers to prevent the sharing of that information with third parties. They are required to give reasonable access so that their customers can correct any inaccuracies with their profile information. And, finally, they must provide reasonable security mechanisms to protect the personal information that is gathered.

The TRUSTe program also incorporates the enforcement called for by FTC and DOC policymakers. Web sites that display our privacy seal must also subject themselves to our oversight and enforcement mechanisms.

There are three essential elements to TRUSTe's oversight process. First, once a site is TRUSTe-certified, we perform quarterly Web site audits to ensure that nothing significant has changed that would impact the site's privacy policy and adherence to our program.

The second oversight element is our seeding process during which we will plant unique data on a TRUSTe-certified Web site to see if that information comes back to us. This allows us to know if a Web site is adhering to its own stated privacy policy.

The third element of our oversight process is our dispute resolution mechanism called the TRUSTe Watchdog. The TRUSTe Watchdog allows Web users to turn to TRUSTe if they believe that their privacy has been violated by a TRUSTe-certified site.

Through these three mechanisms—the Web site audit, the seeding process, and the TRUSTe Watchdog—we are able to catch and resolve most privacy problems quickly and to the satisfaction of the Web user.

Our power to enforce adherence to these standards is derived from a contract that all Web sites must sign as a pre-requisite to displaying the privacy seal. This contract can be upheld internationally making it an effective tool for the Internet. And because we require each Web site to annually renew its contract—and we continually strengthen our requirements—our program remains flexible so that we can keep up with change in both technology and public policy.

At times, though, we are forced to use an arsenal of recourse mechanisms that are built into the TRUSTe program to provide a disincentive to companies that break the rules.

For example, when we have learned that a company has not complied with its posted privacy policy we have taken swift and appropriate action. We have required companies to change their business practices, to modify their privacy statement, and to delete data inappropriately gathered on a subject. At times we have determined the need for added assurance and have commissioned third-party onsite audits—which, incidentally, are conducted at the licensee's, not the consumer's, expense.

While collectively these recourse measures demonstrate the teeth of our program, we have at our disposal additional enforcement tools for Web sites that display a repeated pattern of privacy violation. The final steps that we can take include expelling a site from our program, revoking its use of the TRUSTe Privacy Seal, pursuing breach of contract legal proceedings, and referring the site to the most appropriate governing body.

Despite our *ability* to use this final deterrent, I am happy to report that we have not yet reached the point where it has been needed. Web sites operate in an environment built on reputation and they know all too well the fallout that would result in being kicked out of our program. To date, no Web site has crossed that line. I can assure you, though, that when it happens the Web community will be ready for our action.

Through the core principles of Fair Information Practices coupled with our ongoing oversight process and enforcement mechanisms, TRUSTe is engaging the Web site and Web surfer in a fair conversation about privacy practices. Furthermore, our contractual relationship with Web sites gives consumers power to control what happens to their personal information, allowing them to decide which Web sites deserve their business.

So how far have we come in generating voluntary participation in disclosing and adhering to privacy practices?

Three years ago, many balked at our approach to addressing the privacy problem, indicating that Web sites would never voluntarily abide by a set of privacy practices that were not mandated by law. Despite the critique, we foresaw that the issue would emerge as a source for competitive advantage in the fierce e-commerce marketplace. Our position was clear: we would target the most visionary and highly trafficked Web sites to participate in the program and then watch the masses follow. That is indeed what happened, as earning the TRUSTe privacy seal has become a standard for most reputable Web sites.

To give you an idea of just how far we've come, in July 1997 we had a total of 15 Web site licensees. Today, that number has risen to more than 1,600, with an additional 150 to 200 applications for the TRUSTe privacy seal received each month. Our licensees are located in over 21 countries worldwide and more than 90 percent of U.S. Web users will be on a TRUSTe-approved site each month.

TRUSTe's growth and reach is actually driving increased consumer recognition of our privacy seal. In fact, since mid-1999, a web-tracking company named Nielsen/Net Rating consistently identifies TRUSTe as the most prominent symbol on the Internet.

And if competition is a trailing indicator of success at building an effective framework for addressing the privacy problem, then the introduction of the Better Business Bureau Online program and the Certified Public Accountant's WebTrust program is a clear signal that seal programs work.

But while significant progress has been made, we also understand that we have a long way to go.

Now that we have built a solid foundation, our first efforts moving forward will be focused on consumer education. We fundamentally believe that Internet privacy isn't just an issue about corporate use of personal identifiable information, it is also an issue about consumer education. After all, in the offline world, consumers rarely even had the opportunity to seek out a privacy statement.

We are already off to a good start at consumer education with two successfully executed campaigns. Our first educational effort was the Privacy Partnership, a grassroots advertising campaign aimed at educating online consumers about their privacy rights. Led by an unprecedented union of all of the Internet portal sites, the Privacy Partnership was considered the biggest online advertising campaign for its time. In fact, today more than 1,600 Web sites have joined by donating millions of dollars worth of banner advertising space.

Following on the success of this campaign, we produced an online safety tips video for this past holiday season. The video brought together industry and government, featuring the Secretary of Commerce, the Chairman of the FTC, and a senior executive at Microsoft giving guidance on how consumers could protect their privacy on-

line. Once again, this effort was met with success and serves as a model for efforts moving forward.

Through educational campaigns like the Privacy Partnership and the Safety Tips Video, we are working hard to raise awareness not only to the privacy issue, but also to how consumers can best control the uses of their personal information and protect themselves online.

Our second area of focus moving forward will be on evolving the TRUSTe program to address the fact that personally identifiable data is increasingly being collected in more areas than just the Web site. TRUSTe believes that all citizens should have the right to control the uses of their personal information—regardless of where it is collected.

In the short-term future, we will be taking the next major step forward in online consumer privacy protection by initiating a Privacy Seal Pilot Program that monitors and enforces the privacy practices of software. Already, there is overwhelming interest by the software industry in participating in this program.

Of equal importance to the evolution of our program, is our focus on the safety of the most vulnerable Web users: children. As most of you know, April 21st marked the enactment of the Children's Online Privacy Protection Act. Today, TRUSTe is finalizing its application to the Federal Trade Commission for safe harbor status giving us the authority under the Act for oversight and enforcement.

Clearly, we have big plans moving forward. By evolving our program to cover more areas of the data gathering network, educating consumers about our seal program, and focusing on children's protection, we are demonstrating our ability to not only keep up with technology's changes but *anticipate* them before they happen.

I want to conclude, Mr. Chairman, by thanking you for inviting me here today. Based on TRUSTe's growth and evolution over the last three years, it's clear that seal programs are providing a critical framework for consumer protection online.

To put this progress into context, today's information revolution is most often discussed as a parallel to the industrial revolution. The two periods are marked by America's greatest display of wealth, prosperity, and technologic advancement. But technology has always outpaced consumer protection. The industrial age, for example, gave us significant environmental problems that, decades later, we have only begun to address.

The information age, on the other hand, is ahead of the curve. The industry is addressing privacy, security, consumer protection and children's access in a time frame never before seen. Seal programs, like TRUSTe, were created to expedite a system of standardized best practices. Clearly, we are seeing that we are succeeding in our mission.

But we need to realize that this self-governance framework, like the medium itself, is in its nascent stages.

The vision of self-governance is a result of the democratic quality of the Internet, where the law is defined largely by the engagement and participation of each community member. That requires the participation of all members of the Web community, from the media to businesses to advocacy groups, in educating consumers about their privacy rights online and what road signs to look for on the Web.

It also requires the engagement of public policy decision-makers in scrutinizing the activity of the online world. You can help our efforts by using your influence to urge companies that have not joined voluntary privacy oversight programs, to do so. Once these companies post privacy statements and join oversight programs, we can use existing laws to regulate and enforce their practices.

Based on the initial success of the TRUSTe program and our future course of action, we are well on our way to creating a safer and more consumer empowering environment on the Web.

I would now be happy to answer any of your questions. Thank you.

Mr. COBLE. Mr. Szafran.

STATEMENT OF MARC SZAFRAN, GENERAL COUNSEL, ENTERTAINMENT SOFTWARE RATINGS BOARD, PRIVACY ONLINE

Mr. SZAFRAN. Good morning, and thank you for the opportunity to appear before your subcommittee as it examines on-line privacy and electronic communications. My name is Marc Szafran, and I am the general counsel of the Entertainment Software Rating Board, also known as the ESRB. Established in 1994, the ESRB is the Nation's leading nonprofit, independent, self-regulatory entity providing support services to the interactive entertainment indus-

try. We have been praised by Senator Joe Lieberman as the most comprehensive rating system of any entertainment medium in this country. Today ESRB not only rates software titles, but also rates Web sites and on-line games, reviews video and computer game advertising, and finally, the reason I am here today, provides a privacy seal service that guards the rights of Web users and seeks to make the Internet a secure, reliable and private place to share information and conduct business.

Privacy Online was launched in June 1999 in direct response to the Interactive Digital Software Association's own initiative to establish voluntary on-line privacy practices for its members. As a result, ESRB created a seal program customized to meet industry requirements and the unique on-line business models of entertainment software companies. Companies that join our program must adhere to rigorous requirements. These requirements include a commitment to consumer notice and disclosure, consumer choice, data integrity and security, data access and, importantly, children's privacy protection.

Compliance with the program also requires companies to display our certification seal on their home page, main pages and personal information entry points. Each seal includes a click-to-confirm option that links users to an authentication page on a secure server. This allows consumers to confirm that a site is in good standing and displays a valid seal. This mechanism was implemented to ensure our seal's integrity and guard against misuse or misappropriation, but what makes our seal program effective and meaningful is its oversight and monitoring elements.

Oversight is managed through our Sentinel Enforcement System, which has four parts; first, on-site audits. On-site audits are conducted annually by a staff attorney specially trained in the area of privacy law.

Second, Sentinel monitoring and verification reviews. These are quarterly reviews of information practices performed by trained monitors. These monitors also conduct sweeps for misuse or misappropriation of our seal by unauthorized sites.

Third, Sentinel spot checks. Our monitoring of a company's privacy practices through a process known as seeding; and finally, our consumer on-line hotline, a no-charge reporting system where consumers can easily and anonymously report violations directly to ESRB.

In addition to our oversight mechanisms, we have also implemented incentives for a company's ongoing compliance. These include contractual obligations. Participating companies must sign our licensing agreement. Failure to comply with its terms and conditions could subject a company to any remedy available at law, such as membership cancellation, monetary fines and compensation in the form of voluntary payments to the U.S. Treasury; also, consumer redress.

ESRB requires companies to maintain an internal dispute resolution system to resolve grievances and provide appropriate remedies. If a user is still unsatisfied, the complaint must be directed to ESRB's certified alternative dispute resolution officer.

Finally, Federal Trade Commission referral. If a company fails to comply with its published privacy statement, we can refer that

company to the FTC for engaging in unfair and deceptive trade practices.

I believe ESRB's program offers a model for industry self-regulation that places consumer interest first while still relying on market incentives, not government. The on-line industry is dynamic and fast-moving, but the same cannot be said of the legislative process. Thus the risk of legislation in this area is that changes in the market will always outrun any regulatory regime, but by combining adaptability with stability, self-regulatory programs led by industry and nurtured by government provide the most effective protection for consumers in the on-line arena.

I thank the committee for the opportunity to share these views, and I look forward to working with the courts and the intellectual property subcommittee in the future.

Mr. PEASE. [Presiding.] Thank you.

[The prepared statement of Mr. Szafran follows:]

PREPARED STATEMENT OF MARC SZAFRAN, GENERAL COUNSEL, ENTERTAINMENT SOFTWARE RATINGS BOARD, PRIVACY ONLINE

I. INTRODUCTION

Good morning, Mr. Chairman, and thank you for the opportunity to appear before your subcommittee as it examines issues regarding online privacy and electronic communications. I am Marc Szafran, General Counsel of the Entertainment Software Rating Board ("ESRB") and it is an honor to testify before you today.

The ESRB is an independent, self-regulatory entity that provides comprehensive support services to companies in the interactive entertainment industry. Established in 1994, the ESRB is the nation's leading, non-profit, entertainment software rating body. Although originally charged with developing a standardized rating system for entertainment software, since its inception the organization has grown proactively in protecting consumers and anticipating the evolving industry. Today "after rating over six thousand-five hundred game titles and having been praised by Senator Joe Lieberman as the 'most comprehensive rating system of any entertainment medium in this country'" the ESRB has evolved into a dynamic and effective self-regulatory organization. This organization has established itself as one of the preeminent institutional models for effective and meaningful self-regulation for interactive entertainment. We now provide services not only for rating software titles, but for rating websites and online games, for ensuring online privacy protection, and most recently, for reviewing advertising created by the interactive entertainment industry.

As General Counsel, one of my primary responsibilities is to oversee the operations of ESRB Privacy Online; one of four divisions within the ESRB. ESRB launched the ESRB Privacy Online Program in June of 1999. This launch was in direct response to the Interactive Digital Software Association's ("IDSA")¹ own online privacy initiative. The IDSA had published a voluntary set of principles and guidelines regarding the online protection of personal data for the guidance of IDSA member companies. These far-reaching guidelines were at the forefront of industry initiated, self-regulatory protection for consumer privacy. They contained comprehensive protections regarding children, notice/disclosure, access, security and enforcement. As part of these guidelines, companies were required to procure the services of an independent, third party seal provider to monitor and enforce published privacy practices and provide consumer dispute resolution services.

ESRB's familiarity with the nuances of the interactive entertainment industry and our reputation for helping consumers make educated choices in digital entertainment media indicated that we would be uniquely qualified as a seal provider for interactive entertainment companies. As a result, ESRB Privacy Online was created and customized to meet the unique online business models of the industry. To date, we have certified eight of the nation's leading interactive entertainment software publishers and are currently in the process of certifying an additional six. Collectively these fourteen companies account for 75 percent of the \$6.1 billion in reve-

¹The IDSA is the U.S. association exclusively dedicated to serving the business and public affairs needs of companies that publish video and computer games for video game consoles, personal computers, and the Internet.

nues generated by the industry last year. In addition, we have eleven other companies that have requested our services.

The ESRB Privacy Online Program is an independent privacy seal program that guards the rights of Web consumers, and the interests of Web publishers, and makes the Internet a secure, reliable, and private place to share information and conduct business. From our principles and guidelines for fair information practices, to our Sentinel enforcement mechanisms, I'm confident that you will find we offer a comprehensive, meaningful and effective privacy seal service that can serve as a successful model for Internet self-regulation.

Today I will discuss in detail the ESRB Privacy Online Program, its mandatory requirements, and the services we offer as a seal provider. In addition, I will discuss why seal programs are resulting in effective and meaningful consumer online privacy as the Internet and electronic commerce continue to proliferate. This discussion will cover how: (i) self regulation and the ESRB Privacy Online Program provides effective consumer protection as an alternative to government regulation; (ii) our Program's assessment mechanisms and alternative dispute resolution services operate; and, (iii) these assessment mechanisms and our compliance incentives provide effective and meaningful enforcement. I provide this testimony on behalf of ESRB with the hope that our experience can serve as a model for other consumer privacy protection initiatives and as an example of how industry-led self-regulatory programs can provide true protection for consumers in all areas of the global electronic arena.

II. THE ESRB PRIVACY ONLINE PROGRAM

Participating companies must adhere to rigorous ESRB Privacy Online Program requirements, including accepted Principles and Guidelines for Fair Information Practices ("Principles and Guidelines"). The Principles and Guidelines regulate online information collection and use practices by requiring participating companies to maintain a commitment to consumer notice, consumer choice, data access, children's privacy protection, and data integrity. Compliance with the ESRB Privacy Online Program requires companies to display the ESRB Privacy Online Certification Seal on their homepage, all main pages, and any information entry points where a consumer could disclose their identity or personal information. This ensures that:

- Web users are given clear and simple notice of a site's information practices;
- Web users have options regarding whether and how their personal information is used;
- Web users have reasonable access to information about them collected online and have the opportunity to correct any inaccuracies;
- Web users have assurances regarding the accuracy and security of personal information; and,
- Parents of children 12 and under can decide whether their child's information is collected and how it can be used.

Companies that meet ESRB Privacy Online's high standards are awarded the ESRB Privacy Online Certification Seal—a symbol of integrity and compliance. For the Web consumer, this seal offers an assurance that the site has adopted an approved privacy policy, that its stated privacy practices are being implemented as represented in their policy statement, and that the site submits to ongoing, independent, third-party monitoring and oversight mechanisms. Each Certification Seal includes a "click-to-confirm" option that automatically links a user to ESRB Privacy Online's Authentication Page. The Authentication Page is located on a secure server and provides consumers with the ability to confirm that the site with which they are interacting is using a valid, certified ESRB Privacy Online Certification Seal and that the company is a participant in good standing with our program. This mechanism was implemented to ensure the integrity of the Seal and guard against misuse or misappropriation by unauthorized web sites.

Because participating companies must implement and publish privacy statements that inform consumers about its information practices, ESRB Privacy Online offers services to assist companies in creating or modifying these critical documents. These services include: (i) an online privacy statement composition program called the ESRB Privacy Statement Composer; and, (ii) a Policy/Statement Creation Assistance Team.

If a participating company does not have a privacy statement, the Composer helps a company create their first draft. This draft can subsequently be customized to meet a particular business model and unique privacy practices. The Composer provides companies with the framework for creating a compliant privacy statement that

gives consumers notice regarding information collection practices and demonstrates a meaningful commitment to protecting online privacy.

Finally, with regard to drafting clear, complete and understandable privacy statements, ESRB Privacy Online's services also include the provision of a team of legal and business experts who are trained to help participating companies create compliant privacy policies and statements. The team is available to work one-on-one with companies to ensure that privacy policies and statements contain collection and use practices that adhere to all of ESRB's requirements and that can meet the parameters of most existing business models.

The certification process can be extremely rigorous and demanding for companies in a variety of ways. In many cases, companies are required to considerably modify existing internal practices to meet the requirements of the ESRB Privacy Online Program. From revising customer service procedures, to implementing new technical mechanisms such as online consent forms, creating multi-functional age fields, etc., to modifying existing marketing and promotional models, companies frequently can incur significant costs as a result of coming into privacy compliance. Often database procedures must be overhauled, additional personnel must be hired and trained, new security systems must be devised and implemented. For larger companies, this can be expensive and time-consuming. For smaller, "mom-and-pop" companies, these requirements can be even more significant. Responsible companies however, still realize the long term value of privacy compliance and sustain the rigors of certification to ensure effective consumer protection.

III. SENTINEL OVERSIGHT, MONITORING AND ENFORCEMENT SERVICES

The Sentinel Program is ESRB Privacy Online's enforcement and accountability mechanism; the apparatus that verifies that participating companies comply with their published information policies. The Sentinel Program is broken down into four distinct parts: Sentinel On-Site Audits, The Sentinel Consumer Online-Hotline, Sentinel Monitoring and Verification, and Sentinel Spot Checks.

Sentinel On-Site Audits. Prior to certification, and at annual intervals thereafter, each participating company must submit to an on-site audit. Each on-site audit is conducted by a staff attorney who is trained in the area of privacy law. Through these on-site audits, ESRB Privacy Online determines whether a company's privacy statement is an accurate representation of its internal and external information practices. The on-site audit also provides ESRB Privacy Online with the opportunity to ensure that a company's information practices meet all of our program's requirements and such requirements are maintained on a consistent basis. ESRB will not grant or renew a certification without first conducting an on-site audit and certifying that a company meets the program's criteria. ESRB Privacy Online maintains a record of each participating company's on-site audit for a period of three (3) years.

Sentinel Monitoring and Verification. ESRB Privacy Online also conducts both random and scheduled quarterly reviews of a participating company's information practices. The goal of these reviews is to provide effective ongoing enforcement and assure both the consumer and the participating company that a reliable safeguard exists to verify that a company's privacy policy implementation is accurate, meaningful and effective. Monitoring reviews are unannounced and consist of specially trained online monitors methodically moving through a participating company's Web site, Web page by Web page, URL by URL, ensuring that: (i) a functional link to the participating company's privacy statement is posted on its homepage, all main pages, and at all information entry points; (ii) all personal information entry points include a date of birth field that can determine if a user is twelve years old or under and then activate the information entry point to not collect personal information and instead trigger a parental consent mechanism; and, (iii) comply with all other ESRB Privacy Online Program requirements. Each monitor is required to complete a comprehensive report that memorializes the reviewed company's practices and must archive the site through an actual CD-ROM duplication. Both the monitor's report and the CD-ROM are maintained by ESRB Privacy Online for a period of three (3) years. In addition, monitors are required to routinely input identifying privacy terms (i.e., "privacy policy," "privacy statement," "certification seal," and "ESRB Privacy Online,") into various search engines to ascertain if an unauthorized web site is misusing or misappropriating the ESRB Privacy Online Certification Seal.

Sentinel Spot Checks. ESRB Privacy Online also periodically conducts unannounced audits of each company's privacy practices through planted "spot checks." Sentinel Spot Checks are random, unannounced reviews of a participating company's online information practices through a process known as "seeding." The seeding of a participating company's database is done by a Web monitor who submits ficti-

tious consumer data at each information entry point. The Web site's response is then tracked and recorded to determine if the company's collection and use practices adheres to its privacy statement.

Consumer Online-Hotline. Another effective method for enforcement used by ESRB Privacy Online is the Sentinel Consumer Online-Hotline. The Sentinel Consumer Online-Hotline is a no-charge service that allows Web users who have a privacy grievance or who believe that a privacy violation has taken place on a participating company's Web site to directly report the violation/grievance to ESRB Privacy Online. The reporting can be done swiftly and easily by filling out the Sentinel Consumer Online-Hotline form and indicating on the form the alleged privacy violation. ESRB Privacy Online responds immediately to all consumer concerns and/or complaints (See Consumer Redress below).

IV. EFFECTIVE INCENTIVES FOR PARTICIPATING WEB SITES' COMPLIANCE WITH ESRB PRIVACY GUIDELINES.

ESRB Privacy Online provides effective incentives for a participating company's compliance with its Principles and Guidelines. This performance standard is satisfied by ESRB Privacy Online through the following ways:

Contractual Obligations. To participate in the ESRB Privacy Online Program and post a Certification Seal, a company must first execute the ESRB Privacy Online License Agreement. As part of this Agreement and as a material obligation, participating companies must agree to comply at all times with the Principles and Guidelines. Failure to comply with the Principle and Guidelines could be interpreted by ESRB Privacy Online as a material breach of the Agreement and constitute a trademark infringement and a dilution of the goodwill and reputation attaching to our mark. As a result, this contractual arrangement serves as an effective incentive for participating companies to comply with our Principles and Guidelines. In the event of a breach, ESRB Privacy Online is prepared to pursue a number of remedies, including revocation of a company's Certification Seal, canceling membership status, publication of a violation, the payment of fines, compensation in the form of voluntary payments to the United States Treasury in connection with an industry-directed privacy program; and pursue any other remedies available at law.

Consumer Redress. ESRB Privacy Online also requires that each participating company maintain an internal dispute resolution system that provides consumers with the ability to fairly and expeditiously resolve privacy grievances and receive appropriate remedies. Specifically, each participating company must create a simple, effective system that allows a Web user to lodge a complaint against a participating company. Each company must appoint an identifiable, accessible, and responsive individual who will serve as the participating company's privacy policy administrator. This privacy policy administrator must be given the authority to investigate a Web user's complaint and complete any necessary investigations in a timely manner. If the privacy policy administrator determines that a complaint is valid and/or that the participating company has not adhered to its information practices, the Web user should be offered a remedy. Such remedy must be appropriate under the circumstances of the case and may include the righting of the wrong (e.g., correction of any misinformation, cessation of further data collection from that consumer, or destruction of improperly collected data) or compensation for any harm caused.

If a Web user is still unsatisfied with the resolution of a complaint, or any other aspect of the participating company's internal dispute resolution process, the complaint must be directed to the ADR Officer at ESRB Privacy Online either at the Web user's own initiative or by company referral. At this point, ESRB Privacy Online, under the auspices of its ADR Officer, will implement its resolution processes, including investigations and compliance reviews. ESRB Privacy Online sponsored mediation or arbitration services seek to resolve disputes or complaints within a seven (7) to fourteen (14) day period.

Both ESRB Privacy Online and the participating company must maintain accurate records of any complaints and response to such complaints for a period of three (3) years.

Commission Referral. If a participating company fails to take appropriate actions in response to a valid complaint or an ESRB Privacy Online mandate, or in any way engages in a pattern of violating ESRB Privacy Online requirement's, ESRB may invoke the remedies described above regarding contract breaches and is prepared to refer such company to the Federal Trade Commission for engaging in unfair and deceptive trade practices.

V. THE EFFICACY OF SELF REGULATION VS. GOVERNMENT REGULATION

The global electronic marketplace is in its nascent stage. As such, the e-marketplace requires experienced and capable hands to assist it in achieving its fullest potential. A critical element of achieving this potential is to ensure that participating consumers are protected to the maximum extent possible. ESRB Privacy Online asserts that effective self-regulation is the best way to achieve this goal. This belief is grounded in the fact that the online industry is highly motivated to adapt quickly to marketplace changes and employ meaningful measures that will protect consumer rights. The people and companies that deal with the industry's constant change and unique requirements are those in the best position to guide and refine its development. As all successful and responsible business people realize, consumer protection is an essential element of this development. An online business that cannot assure consumers that their privacy will be guarded is a business that will fail.

For this reason, ESRB Privacy Online believes, in agreement with what the Federal Trade Commission has thus far maintained, that it would be best for government to contain the regulatory impulse and facilitate self-regulation as the proper approach to protecting consumers in the e-marketplace. Government regulation could well obstruct the existing market incentives that have already begun to inspire merchant dedication to consumer protection. Furthermore, governmental regulations are jurisdictionally self-limited. In a global electronic market place, various differing jurisdictions and incompatible regulations will surely generate wasteful conflicts—conflicts between nations, between the federal and state governments, even between the states themselves. The result of these conflicts will certainly be the accompanying protracted litigation of choice-of-law statutes, provisions, and agreements.

Instead of impeding market incentives, government's role should be to encourage and facilitate industry-led self-regulation. To be effective, the online industry requires speed and flexibility to self-regulate the dynamic e-marketplace. By combining adaptability with stability, self-regulatory programs led by industry and nurtured by government provide the most effective protection for consumers in the online arena. Such industry-led self-regulatory programs develop consumer confidence in a variety of ways.

Privacy Seals—Self-regulatory, industry-led privacy seal programs strive to protect the personally identifiable data that consumers may provide when they visit a website. Entities like ESRB Privacy Online, independently evaluate a website's privacy policies to ensure that: (i) such policies comply with recognized principles for fair information practices; and, (ii) consumer data is not being mishandled. Such entities act as a proxy for the consumer, demanding the same privacy guarantees that a consumer would but with greater review and enforcement power than the individual consumer would be able to exercise. As a proxy consumer, seal providers have a vested interest in the transaction with the merchant, but owe allegiance to the consumer. The veracity and reliability of the third party's seal is the sole market influence on the seal provider; if they do not provide effective protection for consumers, they lose credibility and thus effectiveness. It is this threat that prevents third-party seal providers from becoming facades that merchants might use to avoid governmental intervention. As a result, the consumer confidence that is required for a seal provider to operate is the most efficient and effective form of consumer protection in the global electronic marketplace.

Remedies—Not only do self-regulatory seal programs encourage confidence in the global electronic marketplace in their role as guides to reputable businesses, they also provide a mechanism for accountability and recourse. Seal providers like ESRB Privacy Online have a number of remedies available to them that the average consumer does not. Seal providers are in a position to impose penalties on non-conforming merchants. They are also able to exert market pressures on merchants by publicizing the names of non-conforming merchants; a stigma difficult for the average consumer to apply. Seal providers can make use of extensive alternative dispute resolution agreements with the merchants in order to ensure accountability. They can refer non-conforming merchants to applicable law enforcement and administrative bodies, such as the FTC, but with much more intensity than the individual consumer. Finally, seal providers can pursue breach of contract claims against merchants who fail to implement and maintain the requisite level of consumer protection.

Education—Industry-led self-regulatory programs also serve to educate the online community. Throughout the process of certification, both consumers and merchants learn the value of privacy protection. Consumers who learn and have confidence that they can control the use of their own personal information will be less likely to avoid e-commerce for that reason. By removing the most prevalent deterrent to

e-commerce—consumer fears regarding privacy online—independent seal providers stimulate the electronic economy and provide effective protection for consumers. As merchants learn that consumers demand privacy protection, those who want to remain competitive in a burgeoning industry will regard privacy protection as a mere “cost of doing business” online. By providing cost-effective privacy certification services, third-party seal providers like ESRB Privacy Online help reduce the costs of doing business online and encourage greater self-regulation by industry.

Such self-regulation, led by industry with the support of government, makes superior use of market forces and the flexibility of industry to deal with the rapidly evolving nature of the Internet. By assuring consumer control of personal privacy, providing a variety of efficient remedies, and encouraging confidence in the global electronic marketplace through education, independent privacy seal providers such as ESRB Privacy Online will be able to provide the most effective protection for consumers on the Internet.

VI. CONCLUSION

The emergence of the Internet and electronic commerce has brought the issue of online consumer privacy to the forefront of the electronic age. Consumers are increasingly conscious about protecting their privacy when they share information or transact business online. Web publishers are under intense scrutiny regarding online information collection practices. Fear about the loss of privacy is the single greatest obstacle to widespread consumer participation in the electronic marketplace. In the battle for electronic survival of the fittest, the companies that thrive will be the ones that implement and maintain effective, meaningful measures that guarantee the protection of consumer personal information. We believe that the ESRB Privacy Online program is the most complete, cost-effective and comprehensive means to achieve that goal. Backed and administered by the experience, expertise and success of established authorities in self-regulation and the Internet, ESRB Privacy Online provides clarity, support and direction for providing maximum online consumer privacy protection.

I thank the Committee for the opportunity to share these views and discuss these critical issues and look forward to working with the Courts and Intellectual Property Subcommittee in the future.

Mr. PEASE. Ms. Mulligan.

STATEMENT OF DEIRDRE MULLIGAN, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

Ms. MULLIGAN. Thank you. The Center for Democracy and Technology is pleased to have the opportunity to appear before the committee. The issue of privacy is becoming even more pressing, and the Internet is at a critical juncture. While it is only about 10 years now that the Internet has been really a part of our mass media and a part of our individual experiences, I think it is entering a significant transformational time. I believe that this transformation will not occur or not be fully realized if individual privacy is not part of the framework upon which it rests.

CDT believes when we talk about privacy, we need to define what we mean by privacy. Privacy means many things to different people. We like to talk about autonomy, fairness and confidentiality as the bedrock of privacy, and we think that these expectations exist and are important vis-a-vis the private sector and the government. By autonomy we mean the individual's ability to browse, seek out information—picking up your tax forms—without having everyone know everything about you.

Fairness requires that when individuals do decide to provide information to a business or to the government, that it is handled in a way that meets their expectations, it is used for the purpose for which it is disclosed, and if it is going to be used for unintended purposes, that the consumer is involved in that decision and has the ability to accept or reject those terms.

In terms of confidentiality, we believe it is critical to ensure that we have very strong protections for e-mail and other electronic communications. We need to ensure that our fourth amendment is not left behind as we enter the Digital Age.

I would like to refer you to the rest of my written statement for more explanation of these issues, and turn to one specific principle of fair information practice that I think is of critical importance to thinking about privacy and consumers' experience on the Internet today. That is the concept of notice, which Representative Berman brought up earlier today by asking some important questions.

I have a few overheads that I would like to begin with.

As a USA Today story recently found, consumers are often confronted with long, sometimes overly detailed legalese notice statements. In some cases, this is because trying to boil down all of the ways that a company may use data so that it can be read by someone with a 9th or 5th grade educational level is very difficult. At other times it appears that Web sites are trying to confuse consumers.

In the first notice statement, the second sentence says, "with your permission only, we will share information that our merchants request to better serve you."

I am not a parent yet, but I do know as a child, if I had assumed my parents' permission rather than asking them for it, I would have spent an awful lot of time in my room alone. If you read to the third paragraph, they are assuming your permission. It says the information about your order may be shared. If you prefer we not share it, you actually have to object.

Now, my stance would be that for most consumers, the word "permission" means a word that they have grown up with and that they have a specific sense that permission means that they are going to be asked. That is not what we find at this particular Web site.

The second notice that I like to turn to, I like to call, "we won't, but we will." it basically tells consumers, you better read every single sentence on every page if you really want to protect your privacy. It says, "as a general practice, we do not sell your personally identifiable information to third parties." The third sentence says, "however, on particular pages where we ask you for data, we may do something else, in which case those disclosures will override anything to the contrary in this policy." As a consumer, I don't think that would give me a whole lot of comfort. Do I read the policy, read every notice; what exactly should I take away from this?

The final one I would like to examine is what I call "unclear." The first sentence says, "we do not sell, rent or loan any identifiable information." They are not going to disclose it to third parties. It says, "we will not use it in ways in which you have not agreed." But then the next sentence says, "we are going to assume that we can e-mail you," and the next sentence, "we are going to use your name, address and order history for marketing purposes, including sales and geographic analysis." It is not clear to me whether or not consumers have agreed to that or whether it is assumed that they have agreed, and for most consumers looking at these policies, whether or not they can comprehend them is a real question.

I think some sites with privacy policies are doing their best to be direct and clear with consumers. I think there are others, perhaps, who are playing a little loose with language, and at times it may be that they have lawyers who want them to be very, very specific and leave them lots of room.

But notice right now is being overly burdened, and one of the things that would be useful to businesses, to self-regulatory agencies and operations such as the seal programs is some baselines about what consumer expectations are. Notices could then be used to provide consumers with additional information, but there would be some expectation that there are some basic rights and obligations.

In conclusion, thank you, and I look forward to your questions. [The prepared statement of Ms. Mulligan follows:]

PREPARED STATEMENT OF DEIRDRE MULLIGAN, STAFF COUNSEL, CENTER FOR
DEMOCRACY AND TECHNOLOGY

Mr. Chairman and members of the Committee, the Center for Democracy & Technology (CDT) is pleased to have this opportunity to speak to you about the important subject of privacy on the Internet. CDT is a non-profit, public interest organization that is dedicated to developing and implementing public policies to protect civil liberties and democratic values on the Internet. CDT has been at the forefront of efforts to establish and protect the very high level of constitutional protection that speech on the Internet has been afforded by the United States Supreme Court in the *Reno v. ACLU*¹ decision, and to develop sound public policies and technical solutions to protect individual privacy.

Mr. Chairman, the Internet is at a critical juncture in its evolution. Although as a popular mass medium the Internet is less than ten years old, it is already entering into a period of significant transformations. Today I would like to address the privacy issues facing individuals—in their roles as citizens and consumers—on the Internet.

I. PRIVACY

The critical starting point on the privacy questions is the current state of privacy (and citizens' expectations of privacy) and the ways in which the evolution of the Internet may threaten privacy principles. As many of you know, the Center for Democracy & Technology has long been an advocate for protecting privacy on the Internet, and we have previously had the privilege of addressing this Subcommittee on privacy issues. [5] This morning I will briefly summarize our analysis of privacy issues on the Internet.²

CDT believes that a key privacy consideration should be individuals' long-held expectations of autonomy, fairness, and confidentiality, and policy efforts should ensure that those expectations are respected online as well as offline. These expectations exist vis-à-vis both the public and the private sectors. By autonomy, we mean the individual's ability to browse, seek out information, and engage in a range of activities without being monitored and identified. Fairness requires policies that provide individuals with control over information that they provide to the government and the private sector. In terms of confidentiality, we need to continue to ensure strong protection for e-mail and other electronic communications.

As it is evolving, the Internet poses both challenges and opportunities to protecting privacy. The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints could reveal a great deal about an individual's life. The global flow of personal communications and information coupled with the Internet's distributed architecture presents challenges for the protection of privacy.

¹ American Civil Liberties Union v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996), *aff'd*, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

² For a fuller exploration of these issues see, e.g., Testimony of Deirdre Mulligan, Staff Counsel of the Center For Democracy & Technology, Before the Subcommittee on Communications of the Senate Committee on Commerce, Science, and Transportation, July 27, 1999.

II. PROTECTING PRIVACY ON THE INTERNET REQUIRES A MULTI-PRONGED APPROACH THAT INVOLVES SELF-REGULATION, TECHNOLOGY, AND LEGISLATION.

On self-regulation, we must continue to press the Internet industry to adopt privacy policies and practices, such as notice, consent mechanisms, and auditing and self-enforcement infrastructures. We must realize that the Internet is global and decentralized, and thus relying on legislation and governmental oversight alone simply will not assure privacy. Because of extensive public concern about privacy on the Internet, the Internet is acting as a driver for self-regulation, both online and offline. Businesses are revising and adopting company-wide practices when writing a privacy policy for the Internet. Efforts that continue this greater internal focus on privacy must be encouraged.

On the technology front, while the Internet presents new threats to privacy, the move to the Internet also presents new opportunities for enhancing privacy. Just as the Internet has given individuals greater ability to speak and publish, it also has the potential to give individuals greater control over their personal information. We must continue to promote the development of privacy-enhancing and empowering technology, such as the World Wide Web Consortium's Platform for Privacy Preferences ("P3P"), which will enable individuals to more easily read privacy policies of companies on the Web, and could help to facilitate choice and consent negotiations between individuals and Web operators.

On the public policy front, we must adopt legislation that incorporates into law Fair Information Practices—long-accepted principles specifying that individuals should be able to "determine for themselves when, how, and to what extent information about them is shared."³ Legislation is necessary to guarantee a baseline of privacy on the Internet, but it is not one-size-fits-all legislation. Privacy legislation must be enacted in key sectors such as privacy of medical records. For consumer privacy, there needs to be baseline standards and fair information practices to augment the self-regulatory efforts of leading Internet companies, and to address the problems of bad actors and uninformed companies. Finally, there is no way other than legislation to raise the standards for government access to citizens' personal information increasingly stored across the Internet, ensuring that the 4th Amendment continues to protect Americans in the digital age.⁴

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for the individual to correct or amend a record of identifiable information about him.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

The Code of Fair Information Practices as stated in the OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data <http://www.oecd.org/dsti/sti/ii/secur/prod/PRIV-EN.HTM>:

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the sub-

³ Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967) 7. The Code of Fair Information Practices as stated in the Secretary's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, U.S. Dept. of Health, Education and Welfare, July 1973:

⁴ See, Testimony of Deirdre Mulligan, Staff Counsel of the Center for Democracy & Technology, before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, March 26, 1998, at 11-13 (concerning disclosure of subscriber information to the U.S. Navy).

sequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.
5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and, in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.
8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

III. CONCLUSION

The history of the Internet, in general, is that policy regimes are first created by consensus among a broad cross section of the community. CDT is committed to participating in any process that helps to build a new social contract embodying democratic values in the emerging online world. The work of the Federal Trade Commission "through its public workshops, hearings, and its recent Advisory Committee on Online Access and Security" provides a model of how to vet issues and move toward consensus. We look forward to working with this Committee, as well as others, the industry and the public interest community to build a cohesive system of privacy protections for the online environment. Thank you for the opportunity to participate in this timely hearing.

Mr. PEASE. Mr. Zuck.

STATEMENT OF JONATHAN ZUCK, PRESIDENT, ASSOCIATION FOR COMPETITIVE TECHNOLOGY

Mr. ZUCK. My name is Jonathan Zuck, and I am the president of the Association for Competitive Technology, which is a trade association representing over 9,000 companies from all walks of the IT industry that are involved directly in this debate. While their products may differ, they are unified around the notion of preserving the competitive nature of the industry that has allowed this new economy to take place.

I am the token techie on the panel, and so I am excited to be talking about the nuts and bolts of privacy protection. I spent the last 15 years as a software developer and a technology educator and speaking on technology topics all over the world, but never thought that I would be testifying before Congress. It is a great honor to be here. Thank you.

This has been one of the most exciting periods in the history of computer technology in terms of the pace of innovation that is taking place both in terms of technology, but also in the flexibility with which that technology is delivered to the public in terms of marketing models, advertising models and others. So the bottom

line is that the Internet has offered a lot of opportunities for people to get access to information that they might not otherwise have been able to get. It is in that context I urge caution in proposing remedies or regulations that will unduly hamper the innovation that has taken place in this industry.

At the same time, I, like Congressman Berman, would make a distinction between types of information, and there are certainly things like medical records, financial records and perhaps information gathered not on a voluntary basis by the government that should be subject to different standards than straight marketing information being collected on-line, and that is the kind of information that I would like to concentrate on.

I would like to concentrate on three points. One is some of the myths associated with privacy concerns on the Web. I want to talk about some tips and technologies that are available to people today to better protect their privacy on-line, and then also talk about some of the technology that is coming down the pike which should improve that situation even further.

One of the things that has happened as a result of some media blitzes and things like that is that a lot of people have gotten the impression that people can track everywhere you go on the Web, and the reality is that that isn't true. What happens is sometimes some companies get together, perhaps under the auspices of an advertising agency, and agree to share click-throughs or track information within their group, but there is not an external way for somebody to track your progress throughout the Internet, so that kind of invasion isn't possible.

Instead you have a situation where you are trying to tailor information and advertising to particular audiences. So just like you see different ads in Friends than you do during 60 Minutes, you want to be able to track the demographics of the people coming to that Web site because it changes the effectiveness of the advertising on that site. In terms of dollar value, a Web site can collect as much as 40 times as much revenue from an ad that is directed at a particular demographic than one that is generically placed on the Web. That is enough of a difference to make a difference between whether or not that site continues to be free or whether people have to charge for that information. So much like the television model, a lot of this is about keeping information free.

Another thing that has—much to the chagrin of grandmothers everywhere, cookies have taken on dark implications. What used to be one of the most endearing terms of the English language has come to be thought of as this deep, dark portal filed with all of your personal information. I thought we should look at what a cookie really is, and it is not a really very threatening thing. The bottom line is that a cookie looks like this. So as you can see, it is not really full of passwords or any kind of personal information about your finances or anything like that. This is what a cookie looks like, and as threatening as this is, who actually put this cookie on my machine, it was Senate.gov that placed this particular cookie on my machine. I don't feel terribly threatened by this.

A cookie is simply an identifiable number that allows a site to realize that you are coming back to visit that site. So if you have done things to personalize your experience on the site, for example

changed which news you like to see or put in information about what stocks you light to track, that information is stored on the Web site, and that number is enough for them to realize that it is you or that machine that is coming back to that Web site and makes it possible to bring you back to where you were, so to speak, in terms of your experience.

So cookies are not very threatening things, and in many respects they are essential to a smooth experience on the Web, but at the same time you do have flexibility in terms of managing them. You can block cookies, you can do other things to control what kind of availability different sites have for putting cookies on your machine.

So there are also a lot of technologies that are available today. For example, there are wallet programs like Microsoft Password or Digital Me that allows you to store your information in one place and selectively make it available, but have it protected with good privacy policies and strong encryption. There are encryption products that make it easy to protect the information that is stored on your PC and make it more hacker-proof and things of that sort. There are tools that make it possible to remain anonymous on the Web, which is what a lot of people are concerned about. And remailers that allow you send e-mail, but hide where that e-mail had came from.

So there are a lot of existing technology that is available on the Web for people to make use of. Something that is coming down the pike is called the platform for privacy preferences, which is a technology innovation that is going to make privacy policies machine-readable. Your browser, when it gets to a Web site, will compare the privacy policy to preferences you have previously set so if those policies don't match your preferences, the browser warns you and says, "This Web site shares information, enter this site with care." It is sometimes that reminder that is enough to make a difference for users.

The bottom line behind all of these technologies and tips that are available is consumer education, and that is why we started a consumer education campaign and on-line site specifically to educate consumers about how to protect their privacy on-line, and we have placed ads in the *Washington Post* and elsewhere as well on Web sites. So we think that the combination of technology and consumer education will go a long way to address concerns the public, and therefore legislators, have addressed.

Thank you for allowing me to participate.

Mr. PEASE. Thank you, Mr. Zuck.

[The prepared statement of Mr. Zuck follows:]

PREPARED STATEMENT OF JONATHAN ZUCK, PRESIDENT, ASSOCIATION FOR
COMPETITIVE TECHNOLOGY

INTRODUCTION

Good Morning, Mr. Chairman and members of the Subcommittee. I am Jonathan Zuck, President of the Association for Competitive Technology, or ACT. ACT is a national, Information Technology industry group that represents the full spectrum of tech firms—from software developers to IT trainers, from technology consultants to dot-coms, from integrators to hardware developers.

While ACT members vary in their products, they share a common desire to maintain the competitive nature of today's vibrant technology sector that has been responsible for America's "new economy."

It is my sincere honor to testify before this subcommittee today. As a professional software developer and technology educator who spent fifteen years speaking at technical conferences around the world, I am humbled by this opportunity and appreciate greatly your interest in learning more about the technologies being developed today that are enhancing and improving our personal experiences on the Net.

I think I'm the token "techie" on this panel—so I look forward to getting into some of the nuts and bolts of online privacy developments. I think you'll find that there's interesting experimentation taking place on the Internet today that is creating endless opportunities. We're at the very early stages of this worldwide phenomenon—and I urge caution when considering proposals that may hamper the incredible innovation taking place on the Net. I continue to be amazed at the great strides my IT colleagues are making at keeping pace with consumer demands—with privacy protections topping the list.

In my testimony today, I'll help dispel some online privacy myths, provide some tips and tools for online protection, discuss developing technologies and address the implications of patents.

ONLINE PRIVACY MYTHS

The truth is, no one person, entity or service can track everywhere you travel on the Internet. Some isolated events have lead some to believe that it is possible to track everywhere you go on the World Wide Web. This simply isn't so. Instead, what has happened in some cases is that a number of on-line companies, often brought together by an advertising firm, have banded together to share profile information about you in an anonymous fashion. This type of information sharing allows these sites to personalize and tailor your experience to your interests. This is no different than ordering a pair of pants in a catalogue today and suddenly getting lots of clothes catalogues.

One important benefit of collecting profile information about users is the ability to tailor advertising based on that information. On TV, we know that different ads appear during Friends than appear during 60 minutes because the demographics are different. On the Web someone selling advertising on a website can make approximately 40 times as much revenue if they can tell the advertiser about what sort of folks they will reach. Just as with television, this makes the difference between being able to support content with advertising or needing to charge for it. To keep the Internet largely free, we need to take care not to hinder the advertising revenue model.

WHAT'S A COOKIE?

Much of the controversy surrounds a browser innovation called "cookies." Ironically, one of the most pleasant words in the English language has transformed to mean some sort of portal to your most closely guarded secrets. It turns out that a cookie is a fairly simple thing. It is a technology that allows a website limited interaction with your machine allowing that site to store information on your machine for your next visit. Many sites allow you to customize your experience by selecting layout, news preferences, language preferences and favorite cartoons. All of that information is stored on the website and given an id number. A cookie is simply a way to store the id number on the machine so that the next time your machine visits the site, it remembers the preferences. If you look through the cookies on your machine, they almost always just contain a single number, not personal information about you.

So cookies really aren't so bad, but you always have the option of not accepting them. All modern browsers provide some sort of cookie management capability that allows you to turn them off, prompt you before one is saved, or block them by site. This technology works today. There are also several tools on the market to make it easy to read and edit the cookies that are on your machine so you can selectively delete them.

TECHNOLOGY TODAY

Let's face it. Net firms are like businesses in any other sector—they want to stay ahead of the competition and generate revenue. What ACT member companies and IT firms across the Internet realize is that privacy is good business.

Net companies see the same numbers you do which tell them that privacy concerns are a top reason consumers stay away from the Internet. Those who are not yet on the Net skew the surveys we see. Most folks grow less concerned about pri-

vacy risks, the more time they spend on the web. That said, companies know that in order to attract customers, they must offer the kind of privacy standards demanded by consumers and make those policies known. Firms are leveraging the concern into a business-enhancer, and thus a customer benefit — “check out my site, we offer the protection you desire.” Ours is historically a business with unusually low barriers to entry and low switching costs. The software industry has routinely seen as much as 60% market share changes in as little as 18 months. This was at a time when you had to go to the store, buy a new software product, install it, convert your files and learn to use it. Now, switching is as easy as typing in a new location in your browser. There’s literally no site on the web for which there isn’t a viable alternative and folks have shown a willingness to “vote with their mouse” and give their business to those who better protect their privacy.

One interesting example is how Internet service provider Earthlink was able to exploit an unpopular provision of AOL’s privacy policy that required people to “opt out” every year. Their “Opt out of AOL” campaign allowed them to woo a great many AOL users solely on the basis of a superior privacy policy.

WHAT CAN PEOPLE DO NOW?

Sometimes I am asked what can folks do now and, in most cases, the answer is to use common sense. At this point 95% of web traffic is on sites that have posted privacy policies. Once a site posts a policy, the FTC has jurisdiction to make sure they follow it. Therefore, someone surfing the web should check the privacy policy of a site before they provide any personal information and make conscious decisions whether to accept advertising and solicitations from partners of that site. If you don’t find a privacy policy or don’t like the one you find, send a quick note to the webmaster telling him or her that you won’t be providing any information to them until they get in line and then just “click away.”

Another important tip is to guard information like your password, Social Security Number and mother’s maiden name, closely. Don’t give that information out lightly. Ironically, if you ask a hacker how they got a password, most of the time they will tell you they got it by asking for it. No one should ever need to ask for your password over the phone for any reason. It also makes sense to change your password periodically and not to use the same password for every site you visit. Most browsers allow some type of password management making it less necessary to remember your password so you don’t have to pick your dog’s name in order to remember it.

Wallets—MS Passport and kids passport

In addition to common sense, there are some existing technologies to help you. Microsoft Passport consists of two services: a “single sign-in” service that allows you to use a single name and password at a growing number of participating Web sites, and a “wallet” service that you can use to make fast online purchases. There’s only one name and password to remember, and after you sign in to one participating site, you can sign in to others with just one click. You can store information about yourself in your Passport sign-in profile and wallet, so you won’t have to retype it when you visit or make online purchases at participating sites. Your personal information is protected by powerful encryption technology and strict privacy policies, and you’re always in control over which sites have access to it—including your e-mail and mailing addresses. And, when you sign out, all of your Passport-related personal information is deleted from the computer, which means it’s safe to use on public or shared computers.

Kids Passport is a service that helps you conveniently protect and control your children’s online privacy. You can control what information your children can share with participating Web sites, and what those sites can do with that information. In addition, you have the flexibility of making specific choices for each child and for each site, all in one convenient, centralized location.

Internet Security Protection

There are also tools on the market to help protect the information stored on your computer such as Norton Internet Security from Symantec. Norton Internet Security 2000 stops all sorts of viruses, malicious Java™ applets and ActiveX controls, and even hackers before they can access your valuable data. With Norton Internet Security you also get powerful tools to safeguard confidential information on your PC from unwanted visitors. The tools protect credit-card numbers, bank-account information, and other personal data. Norton Internet Security also helps you restrict children’s access to specified Web sites, newsgroups, and other areas of the Internet, and lets you prevent them from submitting personal information through Web forms without your approval. You can even block banner ads, pop-up windows, and other Web page clutter.

Remaining Anonymous on the Web

News groups and chat rooms are not secure. Email from you tells recipients your address. You can use a third-party tool such as ZeroKnowledge to email and do other transactions anonymously. There are sites on the web that allow you to send mail through them so that the recipient doesn't get your email address. This is much like blocking caller id on the phone. These sites are called "remailers" and basically act as junction points when sending mail which scramble the email address of the sender. Most big email spam lists are accumulated simply by seeing who's sending mail in a newsgroup.

You can use a site redirector such as an anonymizer to keep your Internet address from being identified. An "anonymizer" allows you to browse the web without a site being able to uniquely identify you by your Internet address. In the case of people using dial up net access, this is generally not an issue because the address changes every time you sign on. However, many of those with broadband services have fixed addresses making it a decent identifier.

WHAT TECHNOLOGY IS COMING

One of the most interesting technologies coming down the pike is P3P which is an extension of some of the technology that exists today. Sponsored by the World Wide Web Consortium (W3C), P3P (Platform for Privacy Preferences Project) is a framework for products and practices that will let World Wide Web users control the amount of personal information they share with Web sites. It's described as a "privacy assistant." Using a P3P application, a user can enter personal information once and not have to repeatedly reenter it at different Web sites. The P3P application can inform a user of a Web site's practices with regard to gathering and reusing its visitors' personal information. Users will be able to define the information that a specific site can be provided or not provided.

Microsoft already provides a free wizard that allows you to generate a privacy policy that can be read by a browser as well as one which can be read by humans. It is therefore very easy to participate in the P3P movement and become a good actor on the Net. Once the standards have ironed themselves out, it will be possible for a browser to detect the privacy policy of the site you are about to visit and compare it to the preferences you have set. The browser can then warn you of a difference and help you to decide what sort of information you should and shouldn't share with the site. Sometimes, it's just this sort of friendly reminder that is all that is needed to help consumers remain conscious of this issue and protect their information accordingly.

PATENTS AND INTELLECTUAL PROPERTY

Privacy technology adoption is not likely to be hampered by patent protections. The P3P Activity had more to bear than just the policy implications, which was rather new to a body like W3C. It also had to face the problem that participants of early Working-Groups were working on a patent on the same technology. When InterMind Inc. announced its patent claims on P3P-Technology, the Activity stalled for a time. W3C made an investment and ordered an expert opinion on the patent claims from a major patent-law firm. In his outline on the result, Barry Rein explained, why implementing P3P does not infringe the patent of InterMind Inc. As P3P 1.0 contains neither negotiation nor data transfer, there is nearly no risk of infringement of US Patent 5,862,325. In other words, consumers will be able to enjoy the benefits of P3P innovations without impediment from patent claims.

CONCLUSION—AN EDUCATED AND EMPOWERED CONSUMER

In my testimony today, we've hit upon some of the key factors that I see as a software developer and a tech futurist that will play key roles as we develop better and better innovations to provide safe and personal Internet experiences. We've discussed the amazing technologies that are addressing consumer demands and we have heard examples of the kind of market discipline that will weed out the bad actors in the privacy space.

But my organization adds a third prong to our online privacy position, which perhaps is the most important one—consumer education and empowerment.

Industry must do its part to provide the necessary tools and information to consumers so they feel educated and empowered when using the Internet.

To that end I am pleased to draw your attention to www.NetPrivacyPower.org the newest, and I think, deepest site online devoted to educating consumers on protecting their information on the Internet. The site is part of a major, industry-led consumer campaign that hopes to educate consumers on how to protect their privacy

online. It's our belief that this kind of effort will go a long way in addressing consumers' concerns.

The campaign also includes online and offline advertising and direct mail and email all geared toward directing consumers to the site. The response to date has been positive and we look forward to continuing to roll out the effort in markets across America and across the Net.

I thank you again for the opportunity to testify before you today and will be pleased to answer any questions you may have.

Mr. PEASE. Professor Reidenberg.

**STATEMENT OF JOEL R. REIDENBERG, PROFESSOR OF LAW,
FORDHAM UNIVERSITY SCHOOL OF LAW**

Mr. REIDENBERG. Thank you, Mr. Chairman and members of the subcommittee. I would like to commend you for initiating this hearing to look at these privacy issues that affect our economy and our democracy. I always enjoy following a technologist on a panel, since I think it is only appropriate that an academic get the last word.

Let me emphasize four points. The first, I think, responds in part to some of the opening remarks of the ranking member. Data stalking and information trafficking today are routine. These are not a question of anecdotes. The average citizen of the United States cannot read e-mail without Netscape or a third-party learning about it through a Preview Pane or Web bugs. Hidden data profiling techniques is the accepted commercial practice rather than the exceptional transgression of common decency.

I think it is worth pointing out just how readily available data is on the Internet. Marketing euphemisms aside, Acxiom, one of the largest information sellers in the United States with dossiers on 160 million Americans, advertises an ethnic stereotyping system. Acxiom called it an "ethnicity coding system." Acxiom will sell data, and advertises the data essentially as those people who speak foreign, but think white. Student Marketing Group out of California, I believe, offers data on nursery school children that can be segregated by religion.

Today U.S. law does not respond to this information stalking and trafficking. Our laws have not kept up. The harm here is in the misuse of the personal information, and the harm is the lack of trust and confidence for electronic commerce that we have seen time after time in the opinion poll.

My second point is that self-regulation and technology which we have heard about this morning are necessary, but inadequate to protect citizen privacy. They have been great public relations, but lousy as effective privacy. Self-regulation assumes that the marketplace should resolve these issues, but privacy is a political right. It is part of our freedom of association, our ability to interact in society, and typically in a democracy we do not sell political rights.

Even if you do not agree with that, self-regulation has relied on notice, disclosures. We have heard in the previous statements just how confusing these notices are. In effect, the disclosures are legal nonsense for the average American citizen, and privacy is a right for every American, not just those with a law degrees who can figure out what these statements say.

I do not think that the seal programs that we have heard about are a substitute. The seal programs go across the map in the substantive standards that licensees will be applying to personal infor-

mation. The only seal program that provides remedies to the victims is ESRB that we heard about this morning. The other major programs do not. Similarly, if seal programs cover thousands of Web sites, that coverage is a minuscule number of Web sites compared to the number doing business on the Web.

As for the technology itself, technologies are not policy-neutral. Cookies appear to be an innocuous number, but cookies are a surveillance-enabling device. *Business Week* reported earlier this spring that only 30 percent of computer users even know what cookies do. In a society where most Americans cannot program their VCRs, how can we expect the average citizen to understand the privacy implications of Web bugs, dynamic HTML and IPv6?

We heard earlier about the international dimensions with the European Union and that the safe harbor is an endorsement of our self-regulatory approach. I think that seriously misrepresents the European position. In effect, with safe harbor, the Commerce Department is saying that the United States will give legal remedies to European citizens. If companies subscribe to safe harbor, they will agree to a substantive set of standards and provide legal remedies for Europeans, which we do not even require for the protection of American citizens today.

My third point is a recommendation. We need a baseline set of standards. My recommendation is that Congress enact the OECD Guidelines with statutory damages for the misuse of personal information. The OECD Guidelines provide a complete set of standards. They have been endorsed by successive U.S. governments. They have been endorsed by U.S. industry time and again. It is time that we enacted that as a legal standard. They are needed for citizens, and they are needed for U.S. business in the international marketplace.

My last point is that concomitant with enacting U.S. legal standards, we need to have a data protection commission in the United States to promote fair information practices and help U.S. businesses both domestically and internationally deal with privacy issues. Privacy will need constant vigilance, expertise and independent judgment, and it is time that we do that. I thank you for this opportunity, and I would be happy to work with each of you as you consider these issues.

Mr. PEASE. Thank you.

[The prepared statement of Mr. Reidenberg follows:]

PREPARED STATEMENT OF JOEL R. REIDENBERG, PROFESSOR OF LAW, FORDHAM UNIVERSITY SCHOOL OF LAW

SUMMARY

In 1977, the U.S. Privacy Protection Study Commission, reported to Congress that "neither law nor technology now gives an individual the tools to protect his legitimate interests in the records organizations keep about him." Sadly, more than twenty years later, the Commission's conclusion remains equally true today despite the rhetoric of self-regulation, technological mechanisms and sectoral rights. But, electronic communications make the stakes much higher for American citizens and the future of our democracy.

Data stalking and information trafficking are routine in the United States. Technologies of surveillance, data creep and commercial profiling create wide spread abuse of American citizen's right to privacy in personal information. Existing legal rights do not come close to protecting citizens against offensive data practices.

Self-regulation and technical mechanisms are an inadequate substitute for legal rights. In a democracy, privacy is a basic political right that cannot be sold out in the marketplace. In the absence of legal standards, the history of the development and deployment of technical mechanisms does not demonstrate conformity to fair information practices. The failure to assure citizen privacy in America places the United States at odds with the rest of the world and jeopardizes US commercial interests in global data flows.

My recommendations are:

1. Congress should grant U.S. citizens a right to information privacy by enacting the internationally acclaimed OECD Guidelines as a legal mandate with minimum statutory damages for violations.
2. Congress should establish a U.S. Privacy Commission to promote fair information practices in the United States, offer industry a mechanism to obtain assurances of compliance with statutory rights, and represent the interests of the United States at international policy-making bodies.

STATEMENT

Mr. Chairman and Members of the Committee,

I would like to thank you for the invitation to testify and to commend you for convening this oversight hearing on privacy and electronic communications. My name is Joel Reidenberg. I teach information technology law courses, including data privacy law, at Fordham University School of Law and also serve as the Director of the law school's Graduate Program. I appear today as a scholar on data privacy law and policy and do not represent the views of any organization with which I hold affiliations.

My testimony will focus on the lack of citizen privacy in America today and will offer recommendations for legislative action that draw on my research concerning online privacy issues.

In 1977, after three years of Congressionally mandated study, the U.S. Privacy Protection Study Commission, reported back to Congress that "neither law nor technology now gives an individual the tools to protect his legitimate interests in the records organizations keep about him." Sadly, more than twenty years later, the Commission's conclusion remains equally true today despite the rhetoric of self-regulation, technological mechanisms and sectoral rights. Specifically, I would like to make four points:

1. Data stalking and information trafficking have become the norm in the United States.
2. Self-regulation and technical mechanisms are inadequate to protect the inherently political right of citizens to informational privacy.
3. Congress should enact the internationally acclaimed OECD Guidelines as a legal standard and provide minimum statutory damages for misuse of personal information.
4. Congress should create an independent Data Protection Commission that promotes fair information practices in the United States, offers industry a mechanism to obtain assurances of compliance with statutory obligations, and represents the interests of the United States at international privacy policy-making bodies.

Data Stalking and Information Trafficking in the United States

First, the state of American's data privacy is appalling. Data stalking and information trafficking have become the norm in the United States. Within the last eighteen months, Americans have been horrified to learn of Intel's plan to impose a hidden digital fingerprint for the users of every Pentium III chip, of Microsoft's equivalent to a digital social security number secretly emblazoned on files, of DoubleClick's surprise matching of off-line data with hidden collections of online data, and of RealNetwork's surveillance of music listeners. Despite these public scandals, even now, the current version of Microsoft's Internet Explorer (Version 5.0) comes equipped with default settings that facilitate hidden surveillance of users and the current version of Netscape Communicator (Version 4.72) reports back to Netscape every time a user reads Messenger email. In effect, the tendency in the United States is to develop technology that increases data collection and decreases the transparency to citizens of such monitoring.

As a result of increased computing and communications power, previously unimaginable profiles of citizens are now readily available on the Internet. For example, Venture Direct, a New York based company, sells a list of fat black women who

are offered as targets for self-improvement products. Not to be outdone, Acxiom, a company unknown to the public at large, but holding dossiers on 160 million Americans boasted of its "new ethnic system . . . identifying individuals who may speak their native language, but do not think in that manner." Unless I am missing something, Acxiom is essentially offering a list of ethnic Americans who "speak foreign," but "think white." Within weeks of my publicizing this outrageous example at the National Association of Attorneys General last September, Acxiom removed its full data catalog from the company's web. Now, the site merely offers "specialty lists" with a specific mention of the Hispanic market and declines to state clearly that those on the list can even learn of the existence of their profile.

These egregious practices in the business community are just a few examples that offend common decency and represent invidious stereotyping. While industry lobbyists like to say that such practices have not resulted in economic loss to individuals, this argument seriously misconstrues the harm to society from the loss of faith and confidence in the fairness of information practices. The very misuse of personal information is a harm to the individual citizen that calls for redress.

Existing legal rights in the United States simply do not respond to abusive data practices and the need for sanctions against the misuse of personal information. American law is sporadic, confused and wholly inadequate to protect citizens in the face of privacy-invasive technical advances and pervasive online commercial surveillance. The principal statutes protecting American's privacy in the context of electronic communications have simply not kept pace with private sector information processing developments. The Electronic Communications Privacy Act, the Telecommunications Act of 1996, the Cable Communications Policy Act of 1982, and the Video Privacy Protection Act each contain narrow data privacy provisions that do not cover the vast array of online activities. Indeed, Congress has granted drug abusers greater privacy protection than lawful users of the Internet. Even the recent law suits filed across the country in several of the more prominent data scandal cases are forced to rely on deceptive trade practice theories since basic privacy rights are not clearly established in either the common law or statute.

Inadequacy of Self-Regulation and Technological Mechanisms to Protect Privacy

As U.S. industry moved into the business of information trafficking, American public policy decisions continually deferred to industry self-regulation and technological mechanisms for fair information practices. The history of industry self-regulation and technological privacy, however, demonstrates that these mechanisms have not and will not provide effective protection for citizens. These non-regulatory solutions may have been promoted with the best intentions of industry and, most recently, of the Clinton Administration. But self-regulation and technical tools have proven to be little more than public relations and the avoidance of meaningful information privacy for citizens.

Privacy rights mark the boundary between totalitarian and democratic governance. Privacy is central to our freedom of association and our ability to define ourselves in society. These are basic political rights in a democracy and a fundamental American value. In contrast to the political nature of privacy, self-regulation assumes that all privacy values can and should be resolved by a marketplace. Democratic societies do not, however, typically sell off the political rights of citizens. Indeed, Article 1, Section 1 of the California state constitution was amended by referendum to include express protection for privacy and to apply that protection against business gathering and use of personal information.

Reliance on self-regulation is not an appropriate mechanism to achieve the protection of basic political rights. Self-regulation in the United States reduces privacy protection to an uncertain regime of notice and choice. As a set of privacy principles, this misses key elements of the package of universally recognized fair information practice principles such as data minimization, data access, and storage limitations. Self-regulation also enables data collectors to change the rules after the data has been collected from individuals. As a practical matter, most web privacy notices are nothing more than confusing nonsense for the average American citizen. Policies are often found only through obscure links buried at the bottom of a web page and are routinely made 'subject to change.' Once found, USA Today reports that a linguistic analysis of the policies of 10 major sites affected by data scandals shows that readers will not be able to understand the privacy statements without a college education and many could not be understood without a post-graduate education. In fact, privacy policies are practically impossible to draft at a reading level that most Americans can comprehend. Self-regulation, thus, denies the average American citizen an opportunity to make informed choices and reserves privacy for the nation's college educated citizens.

The seal programs are not a substitute for clear independent legal recourse. Seals, at best, offer an incomplete response to the misuse of personal information. Seal programs are inconsistent on the substantive privacy standards that web sites should apply to personal information. Programs such as Truste omit key fair information practice standards from the minimum requirements of certification such as mandatory access to stored personal information. With the rare exception of the ESRB, seal programs do not require as a condition for certification that damage remedies be granted to the victims of information misuse. Seal programs are also unlikely to cover the vast majority of web sites. The two major seal programs, BBBOnline and Truste, collectively certify a miniscule fraction of American web sites. Major sites such as Amazon.com do not even appear to participate.

Furthermore, seal programs narrowly restrict the scope of their certifications in ways that defy reasonable expectations of privacy. For example, Truste only certifies sites with respect to the information that "is used to identify, contact, or locate a person." Yet, Business Week reports that sixty-three percent of Internet users were uncomfortable with web sites tracking their movements even though the sites did not tie the surveillance data with a user's name or real world identity. Seal programs tend only to apply to the collection of data during specific, narrowly defined interactions such as those with web sites. As a result, major data scandals involving Truste licensees such as Intel, Microsoft and RealNetwork turned out to be outside the scope of Truste's certification.

Just as self-regulation and seal programs are flawed, the promise of technology does not work by itself either. In a society where the typical citizen cannot figure out how to program a VCR, how can we legitimately expect the American public to understand the privacy implications of dynamic HTML, web bugs, cookies and log files? The commercial models, however, are predicated on "personalization" and "customization" using these technologies.

Technologies are not policy neutral. Technical decisions make privacy rules and, more often than not, these rules are privacy invasive. For technology to provide effective privacy protection, three conditions must be met: (1) technology respecting fair information practices must exist; (2) these technologies must be deployed and (3) the implementation of these technologies must have a privacy protecting default configuration.

The marketplace alone does not rise to these three conditions. One of the most celebrated technologies, P3P, has been on the drawing board since 1996. Indeed, pressure from European legal requirements was instrumental in moving the standard forward and in affecting the substantive privacy provisions. But, the standard is still only a proposal. Even if the standard is finalized this year, P3P will be useless unless incorporated in web browsers and widely adopted by web sites. And, even if P3P is incorporated in web browsers and widely adopted by web sites, the default configurations may still be set as a privacy-invasive implementation. And even if the default configurations are set to afford maximum privacy protection, P3P offers no means to assure that the practices of web sites actually conform to stated standards. To paraphrase Justice Potter Stewart, "I do not know it when I cannot see it."

Average citizens are in no position to make judgments about the impact of these technologies on their privacy. Despite the widespread press reports about "cookies" technology and the routine deployment by web sites to track site visitors, only 40% of computer users had ever heard of a "cookie" and only 30% of computer users recognize that a cookie is used to track online habits.

In short, self-regulation and technology will not be adequate to assure the public's right to privacy.

Enactment of the OECD Guidelines and Minimum Statutory Damages for Misuse of Personal Information

Congress needs to enact comprehensive legal rights for data privacy. Americans deserve a baseline of data privacy protection and our democracy requires a framework of consistent fair information practices across different types of uses of personal information and processing arrangements. The United States does not need to reinvent the wheel. The O.E.C.D. Guidelines on data privacy were inspired by the United States and endorsed by the United States. These internationally acclaimed Guidelines offer a full set of standards that provide for citizen protection while receiving praise for their sensitivity to business concerns. Congress should enact these principles as a legal standard and provide for minimum statutory damages in the event of violations. With basic rights and statutory damages, citizens will be able to vindicate their privacy without the need for intrusive government oversight.

The existence of a legal baseline in the United States will provide the necessary incentive to stimulate the rapid development and deployment of privacy-protective technologies. With legal accountability, industry will be unable to continue the current practices of data stalking and information trafficking and will have to implement fairly any new technologies that affect citizen privacy.

In the international economy, these legal rights are essential. The United States stands alone among industrialized democracies with its existing haphazard and weak data privacy rules. Although privacy began as an American concept at the end of the 19th Century with Warren and Brandeis' famous law review article, the United States has lost its leadership role in defining privacy at the start of the 21st Century. In contrast, the European Union through Directive 95/46/EC requires each of its member states to harmonize data protection rights for citizens at a high level with a complete set of legal standards. Other countries around the world including Australia, Canada and emerging economies in Latin America are turning to the European model of data privacy for guidance rather than the U.S. industry-driven model. Indeed, the World Trade Organization treaty expressly authorizes our trading partners to restrict data flows in order to protect the privacy of their citizenry. In the absence of stronger legal protection in the United States, US industry is vulnerable to data flow restrictions. The conflict with the European Union over trans-Atlantic data flows is a clear example. Despite the U.S. Department of Commerce's assertions, the safe harbor negotiated with the European Union for data flows to US companies is far from certain to resolve the issue. Whether Europe accepts the deal remains to be seen and there are significant questions about the legality of the deal on both sides of the Atlantic. At the national level in Europe, data protection agencies have expressed substantial opposition to the safe harbor and they will still have considerable latitude in dealing with the United States. Ironically, should the safe harbor become policy, US companies would commit to treating European data in the United States with greater privacy than they would be required to the data of US citizens.

Establishment of a Data Protection Commission

Lastly, Congress needs to establish a Data Protection Commission. The implementation of privacy principles in the dynamic and complex online environment requires expertise, independent judgment and constant vigilance across disciplines and existing agency jurisdictional boundary lines. While the Federal Trade Commission and Peter Swire at the OMB have exercised important roles recently in promoting data privacy, their institutional missions are too narrow for this function. An independent commission offers critical guidance since citizens may undervalue the interests of industry and society at large to information flows and industry will undervalue citizen's privacy.

The roles I propose for the Data Protection Commission are:

- (1) to promote fair information practices in the United States through constant advice and publicity on privacy issues to Congress, industry and the public;
- (2) to offer industry a mechanism to obtain assurances of compliance with statutory rights. Since the interpretation of any enacted data privacy rights will be context specific and may not provide sufficient certainty for industry, the Data Protection Commission should have the authority to issue safe harbor guidance like SEC no-action letters. Such approval would mean that specific practices conform to the legal obligations for the fair treatment of personal information. This safe harbor function should also allow the Data Protection Commission to approve technical protocols, default settings and implementations for their conformity to legal obligations; and
- (3) to represent the interests of the United States at international policy-making bodies. At present, the United States is irregularly represented at critical meetings where international privacy issues and policies are set that affect global data flows.

Mr. PEASE. Your presentations have been very helpful to us. Before we move to questions, I understand that Mr. Goodlatte has an opening statement that he would like included in the record, and we will do so.

Mr. GOODLATTE. Thank you, Mr. Chairman.

[The prepared statement of Mr. Goodlatte follows:]

PREPARED STATEMENT OF HON. BOB GOODLATTE, A REPRESENTATIVE FROM THE
STATE OF VIRGINIA

Mr. Chairman, I would like to commend you for holding this hearing this morning on what is one of the most timely issues facing the Congress today. This hearing actually kicks off a week of heightened activity on the issue of information privacy. Tomorrow Republican House Members will be attending a Members-only retreat on privacy issues in Leesburg, Virginia. I would encourage my Republican colleagues on this dias to attend this informative event. Next week, the Federal Trade Commission will likely be issuing its report on its second survey of commercial websites and the progress they have made in protecting the privacy of consumer information. On Thursday of next week, the Congressional Internet Caucus, which Congressman Boucher and I co-Chair in the House, will be holding its Privacy Lunch Forum in room HC-5 of the Capitol. I encourage all Members to join myself and other Members interested in this issue for an informal lunch and discussion.

But appropriately, Mr. Chairman, these events are preceded by a thorough hearing in this Subcommittee. As the information age continues to grow and develop around us, the protection of that information, much of which is intellectual property, becomes more and more critical. So it becomes all the more important that this Subcommittee closely monitor this and other issues related to the new economy, and I applaud you for continuing to show leadership in this area.

Mr. Chairman, last year at about this time this Subcommittee held a hearing on this subject, where we heard from the Department of Justice and experts working on industry self-regulation proposals that legislation was not needed. I share the concerns of many that as more and more folks are going online, whether at work, at home, or with their children, there is an growing risk of their information being abused by bad commercial actors. I agreed then and I still believe that the most effective way of addressing this problem is through strong self-regulation by industry, working in cooperation with government consumer protection agencies and law enforcement.

At the hearing last year I was interested in determining whether or not a simple disclosure requirement that websites post their privacy policies on their sites would be an appropriate solution to addressing the small percentage of websites that ignore industry self-regulatory pressure and abuse personal information, while still leaving the legitimate commercial websites free to build on the progress they had made in selfregulation. My questions were quickly dismissed, however, as witnesses for the most part determined that the progress being made by industry made even a disclosure requirement unnecessary.

One year later, we find that the many-headed Hydra that is the Federal Government has awoken to the issue of online privacy. From the Federal Trade Commission to the Commerce Department to the Department of Health and Human Services to the Treasury Department to the Congress to the presidential candidates, it is accurate to say that privacy is a hot issue. The progress that we recognized and congratulated last year is but a distant memory. In its place are isolated examples of industry abuses that, while few in number, have been pounced on by the media and that have fueled the fire of advocates of strong federal legislation. The 1998 Georgetown study that showed such progress by industry is about to be replaced by a second FTC study that we anticipate will have mixed results.

Coincidentally, these results will coincide with a push by the White House for strong online consumer privacy protection legislation. At the same time, advocates on the Hill of strong regulation have recently joined to create a "Privacy Caucus." In addition, the European Union and the United States have recently reached an agreement on "safe-harbor" principles that companies will have to adopt in order to prevent a disruption in the flow of data from Europe to the United States. The adoption of these principles by industry will inevitably affect the debate over the degree of industry opposition to implementing privacy protections.

So it seems that the debate has shifted. While many of us continue to believe that industry selfregulation is the only real solution that will be successful in protecting consumer information, we see that industry is no longer united against legislative solutions: Proposals to implement disclosure requirements or create commissions to look at the issue are gaining support among industry participants. However, these proposals are now dismissed by advocates of legislation as too little, too late.

With November 7th just six months away, it's anybody's guess what we would end up with if Congress took up privacy legislation. I think we would all agree that at the end of the day, any final law on privacy would be unlikely to be limited to a simple commission or disclosure requirement. A legislative light touch is hard enough to accomplish without being in the middle of what is arguably the biggest election year in a generation.

So where does that leave us? I look forward to hearing from our witnesses this morning about what they believe the state of play is on online privacy, and what, if anything, they think Congress should do about it. In particular, I would like to hear a convincing argument from the advocates of industry self-regulation as to how they would solve the problem of the small percentage of websites that misuse consumer information. I would also like to hear from the supporters of privacy legislation why, following Congressional action on medical privacy, financial privacy, and children's privacy protections, and at a time when those regulations are still being crafted and implemented, and when the success of those regulations is questionable, we need to jump ahead and legislate over those new laws and create even more new laws and regulations.

Again, I look forward to hearing from our witnesses this morning, and I thank the Chairman for holding this hearing.

Mr. PEASE. Mr. Berman, the gentleman from California.

Mr. BERMAN. Mostly this is to Professor Reidenberg. Touch for a second what is this right to privacy? I have told this story a couple of times just in my office. Political politicians running for office have a tremendous interest to know a variety of information about their voting universe, things like ethnicity, age, perhaps place of birth, because as a general proposition in a world where we attack stereotyping and profiling, the fact is that sometimes you can draw politically effective conclusions based upon those stereotypes, and when it gets right down to winning the campaign, you do all of this. So you tailor your message based on voting affidavits and ethnic surname indexes and cross-referencing with professional directories and forget the whole role of computers. You could do this—if you have enough people, you can do this one by one. Am I invading a constituent's privacy when I do that?

Mr. REIDENBERG. Let me take that in the sense that you seem to be asking whether the data should be out there, and I do not think that is the issue. The issue is that citizens should have a right to participate in decisions about how their information circulates. Yes, of course, there are useful and legitimate uses for ethnic lists and products like that. But I think the citizens on those lists ought to be able to know that the information is circulating and have a right to say whether they should participate in it. Much of the information is coming from private sources as well as public record information.

Mr. BERMAN. Well, the fact is that we have eliminated—between my first race in 1972 in California, we eliminated certain provisions that were on the registration affidavit like place of birth and things like that, but at the end there is not too much that any individual can do to stop me from making ethnic surname conclusions about their name. Maybe we have people register by these numbers or something like that.

I am trying to understand this issue of access to information. It is obviously very sensible to exercise your right to control what information is out there about you and who it goes to, but the question remains: What constitutes—if the information is out there—an invasion of privacy. Is something that is done after that that becomes the invasion of privacy?

Mr. REIDENBERG. It is how the information is collected and used. The OECD principles are very basic. They state that data should be collected lawfully and fairly with the knowledge and consent of the data subject. The data should be relevant for the purpose for which it is being collected. The data should be used only for that

purpose unless there is consent. There should be security safeguards. There should be openness in who is using personal information and how it is being used, and individuals should have the right to obtain from a data controller the information that is being held about them and, if it is wrong, to correct it. And those controlling personal information should be accountable.

Mr. BERMAN. Department stores, when you apply for a credit card with them and they send you information about sales, are they taking information which has been gathered about you and violating OECD guidelines by creating mailing lists where they send you information about sales?

Mr. REIDENBERG. I think that depends on what they tell you when they collect that information. If all they say is, give us all of this information to get a credit card, and the collection is for the purpose of getting the credit card, and they turn around to send you marketing, yes, I think that violates the privacy rights of that individual.

Ms. MULLIGAN. I would like to go back to your first question about the political context. I think you are highlighting a very important issue, and it is an issue that is—if you think about privacy as the ability of individuals to control information that they have disclosed to someone else in a limited setting, and add some of rules which are supposed to limit discrimination, sometimes that information is not data that I have to provide, the color of my skin, my sex, so as you said, it is obvious I can't keep you from making assumptions, but we say you can't use that kind of information to make certain decisions.

Mr. BERMAN. Police using racial profiling?

Ms. MULLIGAN. Exactly. One of the things that I think you are highlighting is that there are other ways that you can use that data that are not perceived as being harmful. It may actually be data such as my name which I am making publicly available in the phone book, or it is voter registration records which are going to be available to politicians, and you can make decisions about Deirdre Mulligan, you have some sense of my ethnicity.

Mr. BERMAN. You are Armenian.

Ms. MULLIGAN. I am Armenian. We are starting to see rubs between what we consider "yucky" uses of data, even though we might accept that some of that data is freely available in the economy for sometimes useful purposes, and that is a narrow segment. Some of the political use of data in the political contexts relies on data knowingly made available to politicians for specific purposes such as running your races.

Mr. BERMAN. It is politicians who write the laws on what is available to politicians.

Ms. MULLIGAN. And you will find that there are very few rules in this particular area. I think what Professor Reidenberg was highlighting, is that we have these fair information practices in general, and they have been broadly accepted. They are—despite other suggestions they are of U.S. origin. They are home-grown and domestic. It doesn't mean that you can take a set of principles and blanketly apply them without appreciating the complexities of a specific area. And it means that there are areas where important societal benefits are going to come head to head, and you are going

to have to make decisions and say, we are going to make certain information available for these purposes because we think this is as important. But what is really important is that we start with a presumption that these fair information practices that this notion that individuals have some decisionmaking power over their data—is the central point.

Mr. BERMAN. Mr. Chairman, Mr. Zuck seemed to want to respond.

Mr. ZUCK. I guess my first reaction as somebody coming out of an industry that moves as fast as the computer industry does, it is important to draw distinctions between the nature of privacy and a society and specific practices within the Internet, for example. If you talk about things like opt-out, it is actually easier in most cases to do that on-line than in the context of catalogs or political information or government information which is getting shared as part of the census. Just as the Internet can increase the efficiency, it can also increase the efficiency on how choices are made. So it is important not to treat the Internet as just a reason to have a broader discussion, but to, I think, be specific and not undermine what has been a very experimental and innovative marketplace.

Privacy is a right and a commodity. Just as people are willing to trade their eyeballs for programming on television, they are willing to trade information for free access to information on the Internet. In the absence of those kinds of available models, we are going to see a situation in which that information ceases to be free. I think the bottom line is about opt-in versus opt-out, and people generally don't care. If you ask people to opt in, then about 15 percent of the people will opt in. If you ask people to opt out, about 15 percent will opt out. It is apathy, et cetera. But it is also essential to the continued free nature of the information on the Internet and I think it is important that we not put overly restrictive and prescriptive regulation in place that might hamper that innovation from continuing forward.

Mr. PEASE. The gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Ms. Mulligan, the argument has been made that a simple disclosure requirement would cause a reduction in participation in the seal programs. I wonder if you agree with that statement.

Ms. MULLIGAN. I think there is a risk in setting a baseline through a legislative process that is lower than something which has been adopted by the good actors in industry. And if you look at the history of privacy laws, whether the Fair Credit Reporting Act or the Video Protection Act, you will find that they attempt to codify best practices, that requires that you at least set a bar that is as high as the best that is going on in the field.

I would be quite hesitant to support something that didn't at the very least codify some of the work of my colleagues. That said, as Professor Reidenberg pointed out, there are some areas where the seal programs need to be strengthened, and I think it is important to continue to work with them and sometimes push on them to see those standards raised.

Mr. GOODLATTE. I am looking at an article from CNET News about the ongoing case against Amazon.com for violating the Consumer Fraud and Abuse Act and the Electronic Communications

Privacy Act. Do you think that the courts are an effective means of encouraging compliance with not just the law, but encouraging affirmative action to seek out and comply with the seal programs?

Ms. MULLIGAN. In general I would say no. One of the things that is actually troubling, if you look at privacy laws, it is not even clear whether or not the remedies are sufficiently available to consumers if they act upon them. Professor Reidenberg talked about a commission. If you look at other countries models, they often encompass something which is closer to a consumer protection dispute resolution procedure where they don't force consumers to bear the cost of going to court, which can be exorbitant in terms of time and economic costs hiring a lawyer, et cetera.

I think there are certainly—the ability to go to court and pursue legal rights is an important piece of enforcement, but for a consumer who feels like their data has been misused and what they want to do is get off somebody's list, you need to have some small claims court, some Better Business Bureau and some other low-cost access points that allow consumers to have their needs addressed and allow business to take care of consumers' needs in a cost-effective manner.

Mr. GOODLATTE. So passage of a disclosure requirement while keeping in place existing laws should not decrease the pressure on Web sites to use seal programs?

Ms. MULLIGAN. I think that it may, because if you set a baseline, and there are businesses who will feel inclined to do more.

Mr. GOODLATTE. If you would offer to take the opposite approach and set up a massive Federal bureaucracy to oversee a privacy policy, and have enforcement mechanisms for each and every one of millions of Web sites in the United States, would that not be a strong disincentive for anyone to participate in a program of a voluntary nature like TRUSTe or BBBOnline because they no longer need that, they have a government route?

Ms. MULLIGAN. I think with the passage of the Children's Online Privacy Protection Act, (OPPA) additional seal programs sprung up or the seal programs that exist actually developed child-specific seals. It did not hinder the development of seal programs. OPPIA provided an incentive for people who needed guidance.

Mr. GOODLATTE. That is different from what professor Reidenberg is calling for, which is setting up an entire agency to go ahead and do that.

Ms. MULLIGAN. I am suggesting that there may be a position in between, and that I think the Children's Online Privacy Protection Act—I think the notion of crafting privacy protections that are based on fair information practices, and ensuring that those are the baseline in the marketplace, and allowing, for example, the Federal Trade Commission—they could be an independent piece of legislation—you could go about this in different ways without—Congress has been not too inclined on establishing new bureaucracies, but I think there is some middle ground.

Mr. GOODLATTE. Mr. Szafran?

Mr. SZAFRAN. I think the issue is whether that is necessary legislation, and I really don't believe it is. Survey after survey has come out which says that the number one obstacles to Web users participating in electronic transactions is their concern over privacy.

There is a recent Forrester survey which came out that said last year on-line Internet retailers lost \$2.8 billion worth of sales as a result of Web users' concern about privacy.

The question that comes up here is if we understand the economics of the Internet, if we look and see, at this point particularly, what has been happening with stocks and the entire industry, the smart actors out there, smart businesses who want to survive, who are there to make money, and this is where the companies really listen and pay attention, that they will do practices which are intelligent practices for surviving.

It is no longer a philosophy of good business practice to put a published privacy statement. It has now become an essential part of the successful business model. Companies that don't give privacy statements on their own will not survive out there.

So in response to your question, I think the answer is that is unnecessary legislation, because there is market incentives out there which will only grow more powerful, which will result in the posting of privacy statements and giving consumers adequate notice.

Mr. GOODLATTE. Could you say something about the benefits of having this data available to the vast majority of people who have been pointed out from various surveys are not going to take a step one way or the other, they are going to bypass that policy page? What kind of benefits are they receiving by having information available to the people that they are doing business with?

Mr. SZAFRAN. I am not sure that it is necessarily true that Web users are going to bypass privacy statements. I think the Internet is in its early stages of development, and I think as the public becomes more and more aware of services such as seal provider services, they will be more apt to look at privacy statements. It is true that there are privacy statements out there that are convoluted.

Mr. GOODLATTE. Would you say that the 85 percent of consumers who would not exercise an opt-out policy are doing so consciously because they know of the benefits of lower prices and having information directed to them that is useful to them?

Mr. SZAFRAN. I think it is a matter of education. As consumers become more aware, they will exercise their choices based on privacy statements.

Mr. ZUCK. I am not sure that 80 percent of people are aware of the benefits that they are receiving, but I think they are balancing what level of concern they have about their on-line privacy, because it is not like news of that is absent in the media or something like that when they make a decision not to worry about a privacy policy.

But the marketplace can impose severe discipline on even good actors who slip up. AOL had a perfectly good privacy policy that you could opt out of, but required that you opt out of it every year. And Earthlink, through a program that they called Opt Out of AOL, was able to gather thousands and thousands of AOL customers because of one change in a privacy policy.

So some people are conscious of it. The market exploits that consciousness, and privacy becomes good business and essential business, as we discussed. I think that with over 59 percent of Web traffic going through sites that have Web policies now, probably the

need for legislation to mandate having a privacy policy probably isn't necessary.

Mr. GOODLATTE. Professor Reidenberg?

Mr. REIDENBERG. A couple of comments. Perhaps my remarks, oral remarks, were a little too cryptic on the Commission proposal. It is not a proposal for a heavy-handed regulatory agency in any way. I elaborate more on the idea in the written statement, but essentially my proposal is that we have a commission whose role is very much to be vigilant and give publicity to information stalking and trafficking activities; educate Congress, the public and the industry of what the issues are; and for industry to provide, in effect, the equivalent of what we see in the SEC, the no action letters, which would essentially be a mechanism for the Commission to say—industry could come to the Commission and say, this is our practice, and this is our code. Is this satisfying our obligation?

Mr. GOODLATTE. The top 100 companies that do business on the Internet have very, very effective, good privacy policies that are based, as Mr. Zuck points out and Mr. Szafran points out—based upon their reputation, their desire to serve those consumers. What we are talking about is literally millions of people with Web sites, some of whom are on the margins not only of electronic commerce, but on the margins of society in terms of their political viewpoints and so on, and it is those people that we are trying to address when we talk about having some kind of a minimum standard. But it is also those people that we are concerned about when we talk about are you going to try to standardize and homogenize, so you wind up increasing the role of government dramatically in the process.

They are not going to come to anybody to say, here is our industry policy; will you give it a governmental seal of approval. They are going to be out there doing all kinds of things with private information, and we have got to do a job of educating the public about the risks that they are exposed to in traveling to any old Web site on the Internet, and are we going to have some kind of a minimum standard that says when you do that, you are subject to some kind of governmental response if you don't meet a minimal requirement, but you are not going to get into dotting the Is and crossing the Ts and how large the lettering has to be and whether it is on your first or second screen.

Mr. REIDENBERG. I am proposing that we have a basic standard that these small Web sites should know what they ought to do. I think it is a problem where only those Web sites with an army of lawyers can deal with privacy issues, and the small businessman out there doesn't and can't. The Small Business Administration has a model.

Mr. GOODLATTE. These are just individual citizens which are occasionally selling a product on eBay or advocating a political point of view or communicating with their friends, but all of those people are subject to using the same technology to potentially invade somebody's privacy depending on how we define what privacy is. This is way beyond what the largest companies in the country might do, in fact are doing, to protect privacy. This is about having some kind of a minimal standard for people who are just average, ordinary citizens, who are not going to have—not even think about

having a lawyer involved. Are we going to have a massive regulatory scheme to dictate how they proceed?

Mr. REIDENBERG. That is not what I am suggesting. I am suggesting that we have a minimum set of standards, which are—the OECD guidelines are that minimum set of standards.

Mr. GOODLATTE. I would think that a lot of people would beg to differ. They go well beyond minimal.

Mr. REIDENBERG. Every successive administration has endorsed them, and the largest companies in the United States have endorsed them as the standard for treating personal information.

Mr. GOODLATTE. We are in a different environment than you are when you are talking about catalog sales or any kind of traditional type of business transactions when you are talking about the Internet. You are not talking about just the largest industries in the country. You are really talking about everybody having to comply with something that they are not going to have the slightest clue what you are talking about.

Mr. PEASE. I hate to do this, but Mr. Goodlatte has used his time and my time, and we do have a schedule to meet. If we have a few minutes after I have concluded—

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. PEASE. Mr. Szafran, you make reference to one of the practices that you use to ensure compliance, and that practice you referred to as seeding. Can you give us a better understanding of what that practice is?

Mr. SZAFRAN. Sure. We have on-line monitors who go to Web sites at unannounced periods during the year. It happens once each quarter, and they will put in fictitious information. There will be an address. That address gets entered into the registration form or whatever the data entry point is on the Web site, and then we will track and see with the information that we have given. If we see that telemarketers are calling a particular number or that we are receiving certain unsolicited advertisements in the mail to this address, we know that there is a violation, and we can pinpoint where it is coming from based upon the Web site where we have entered that information.

Mr. PEASE. Thank you.

Ms. Mulligan, you made a reference, and I have not reviewed your written statement, and if it is there, tell me to read the paper. But you made reference to fourth amendment concerns. Can you go into greater detail?

Ms. MULLIGAN. There is some information in my written statement, and there is reference to a longer statement I prepared earlier this year.

The fourth amendment has been read by the Supreme Court to protect data in your home or in your own computer. As data migrates further away from the home for example, records of the books you purchase, or records of the groceries you buy as that data begin to be stored and detailed and tied to your identity and held by third parties, whether they are out on the network, or at a server, don't have the same fourth amendment protections. That means if law enforcement or a private party wants access, legally they don't have to come to you. You get no notice. They don't have to have a court order or some other kind of judicial process, so a

third party has not said that law enforcement can get access to those records in general. So as a citizen you have limited rights.

As more and more of our data, for good reasons, migrates out on the Net, as you take your wallet and put it on-line because it is convenient, but it is on a third-party server, the consumer's expectations of that data being very, very secure become very misplaced, and we think that we need to ensure that expectations, particularly confidentiality vis-a-vis the government and eavesdroppers and interlopers, and as much as self-regulation might be useful in other areas. This is an area for law and congressional action.

Mr. PEASE. Just a quick follow-up. Some States have laws on access to public information that require when a third party attempts to access information from a government entity, the government entity has to advise the individual whose records are being requested, and that would otherwise—or, in fact, may be publicly available, but still to give them notice that this has been requested. Is this the kind of approach that you think is feasible in this kind—in this context, or are you looking in another direction?

Ms. MULLIGAN. The notice component is a critical one because the problem for an individual is if they don't even realize that somebody is trying to access data, they have no ability to object to it. Notice provides them the knowledge that somebody is trying to get information about them even though they may not have the ability to parent it. In those instances you've described it may be because a police officer or a woman who has been battered, and has safety concerns, are receiving notice ahead of time.

But the important part besides notice is ensuring that data, data held by a business, for example, is only accessible when a standard is met, and that this be a probable cause standard. It is a standard that this data is relevant for what is going on, that there isn't another way to get it. So it is notice, and it is also creating legal standards.

Mr. PEASE. I am sorry for the abbreviated nature, but we have a series of votes on the floor.

Professor Reidenberg, I think I heard you say under the safe harbor provisions that the result could well be that residents of the EU have greater protections than do residents of the USA. Did I understand you correctly, and if so, can you explain that more fully?

Mr. REIDENBERG. That is correct. The European Union has been insistent that any safe harbor text provide substantive standards for how the personal information of EU origin should be treated and that there be legal remedies in the United States for the individuals whose interests—whose information might be misused. The safe harbor proposal—and it has still not been accepted by the European Union, and there is some question whether or not that will occur at the end of this month—the safe harbor proposal sets out a baseline set of standards that American companies can voluntarily subscribe to if they wish to receive information coming from the EU. So in essence—and if they subscribe to it, they are subject to legal sanction in the U.S. either through FTC enforcement—which is interesting that the FTC would be protecting foreigners' privacy perhaps more so than American privacy. So it would be subject to FTC enforcement.

The bottom line is a set of standards and legal enforcement if those standards are transgressed. That is the model presented to Europe. That is not presently the model that the United States has.

Mr. PEASE. Howard is twitching here. Do you want to say something before we close?

Mr. BERMAN. Tell me the Web site operator who would have a privacy policy that he would only show to people coming on that site from the EU?

Mr. REIDENBERG. Safe harbor, in certain countries in Europe, would not apply at all because there is a choice of law provision in the directive that says if the Web Site collects data directly from a user in the European Union—

Mr. BERMAN. If they are doing a privacy policy and disclosing it to the EU, they are going to disclose it, aren't they?

Mr. REIDENBERG. I'm sorry?

Ms. MULLIGAN. There actually are Web sites that have across the bottom, pick the country from which you are coming. Not only will you find that the language, text changes, but the privacy statements change. And in the future I think you will see that happening based on IP addresses.

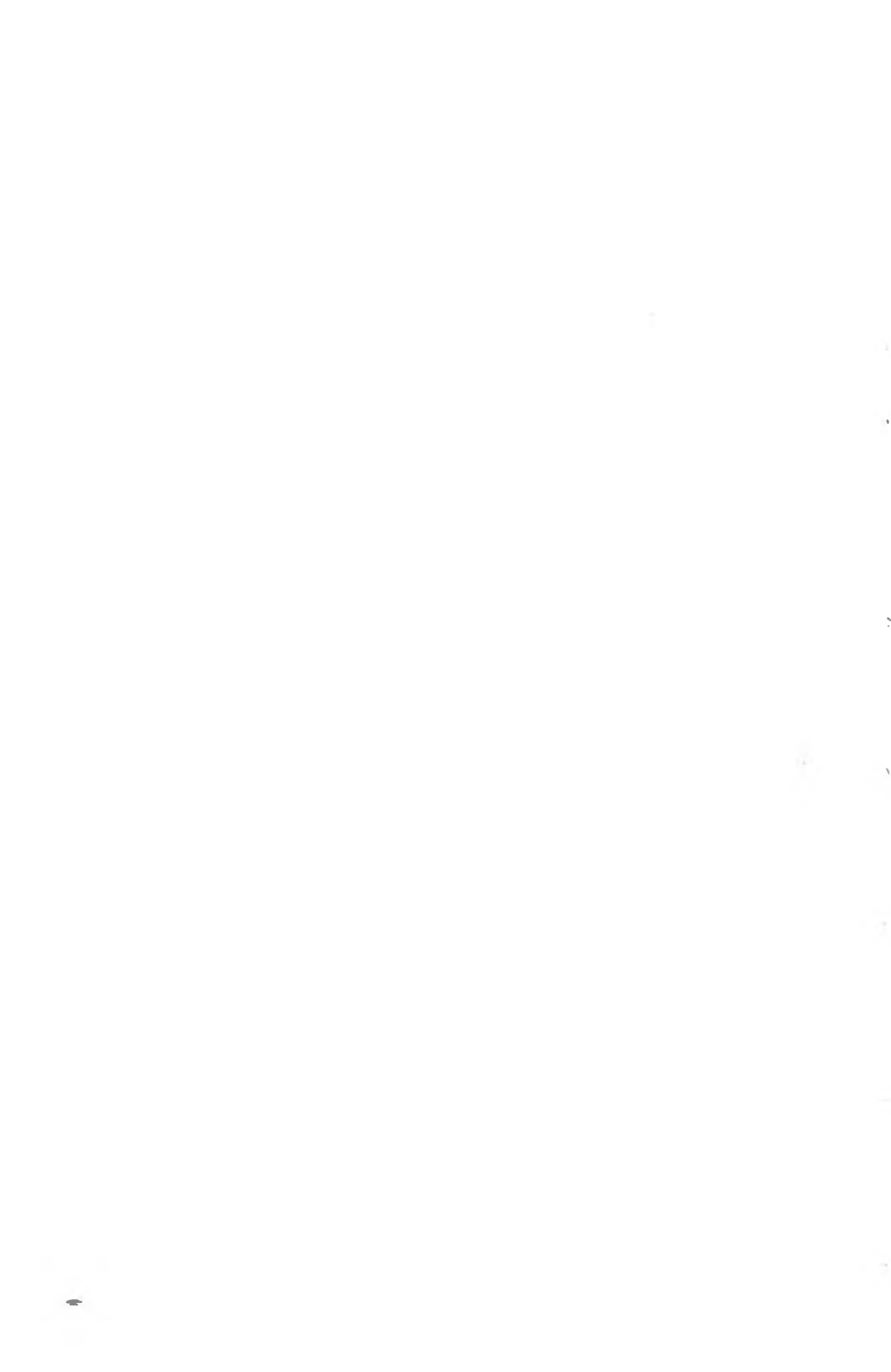
And I wanted to harp on something that professor Reidenberg said. In fact, the negotiation between the U.S. and the EU explicitly states that the Federal Trade Commission will pursue complaints by EU citizens first. And I think that there is something quite troubling, the notion that U.S. taxpayer dollars at a Federal agency are going to be expended in a way that protects the foreign citizens' rights before they protect U.S. citizens.

Mr. GOODLATTE. This is all very interesting, but the fact of the matter is that studies show, notwithstanding the European privacy directive, that U.S. companies have a far higher percentage compliance with privacy standards than do the major European companies, and self-regulation is indeed working in that respect. And the fact of the matter is that the request for the Federal Trade Commission to take care of their citizens on this issue is, I think, a reflection of the fact that we are doing a better job of it than they are.

With due deference to the professor, the politicians get the last word here, not witnesses.

Mr. PEASE. Before I lose complete control of this hearing, thank you. This hearing has raised more questions than it has answered. That is not surprising, but I am very grateful for the information that you have included on this. The record will remain open for 1 week. Thank you for your cooperation. The subcommittee stands adjourned.

[Whereupon, at 12:56 p.m., the subcommittee was adjourned.]



APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD



we won't
but we will

we men.com

How We Use and Disclose Your Information

As a general practice, we do not sell your personally identifiable information to third parties. So, for example, we do not sell your email addresses or your name and demographic information to third parties.

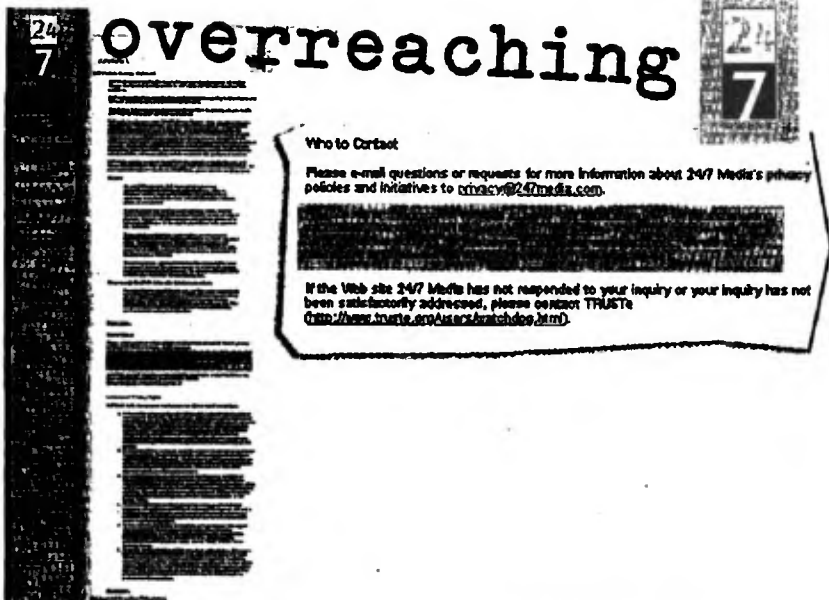
For example, before you submit answers to questions we ask in an advertiser-sponsored promotion, we will tell you that your answers will be shared with that advertiser.

confusing

CatalogCity.com

The personal information you have provided us and information about our products and services that we collect. This information may be used for a variety of purposes. This information will be used to make our future marketing efforts more efficient. It may also be used by our marketing partners to bring you offers of interest. To learn more about our marketing partner, please click www.netdeals.com.

If you agreed to receive email from our marketing partners, we will share with them your email address and the information described above, so they can send you offers for products and services that may be of interest to you. We will only share your e-mail address if you have opted in by checking the box on the registration page. Additionally, each email our partners send you will include a description of the simple opt out process to enable you to stop receiving future e-mail.



OFFICE OF THE DIRECTOR,
BUREAU OF CONSUMER PROTECTION,
Washington, DC, July 10, 2000.

Hon. HOWARD COBLE, *Chairman,*
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR CHAIRMAN COBLE: Thank you for forwarding Representative Edward Pease's question about the public disclosure of personal information by genealogy Web sites raised during the May 18, 2000, Courts and Intellectual Property Subcommittee hearing on "Privacy and Electronic Communications." In response to Congressman Pease's question, we reviewed a sample of genealogy Web sites and the personal information available at these Web sites. The genealogy sites we reviewed can be divided into three categories: (1) *dot com sites* that offer free or fee-based research services and access to information databases; (2) *dot org sites* that provide similar services; and (3) *family-created sites* that document their genealogy. On sites offering free access to their databases, we searched to determine whether they provide information about living individuals. Where sites charge fees for database access, we reviewed the database titles to determine if they were likely to contain information about living individuals.

Except for family created Web sites, most genealogy Web sites we visited do not currently post personal information about living individuals but rather provide historical data. Many of the sites, however, appear to allow users of the sites to add personal information about living individuals to their historical databases. Only two of the sites reviewed provide any cautions or restrictions against posting personal information about living persons.¹

In addition, some of the Web sites we reviewed provide access to public databases containing birth, marriage, and yearbook records. It is likely these historical databases will be updated so that records about living individuals will be easily available.

¹ Familyhistory.com has a user agreement stating that in posting information, users must not have violated another person's privacy, must ensure that the posted information is accurate, and are solely liable for consequences of posting information. Familysearch.org has a user agreement that states users should receive permission from living individuals before posting information about those individuals.

There are currently no federal laws which would limit the collection or posting of information about living individuals on genealogy sites.² The Commission may, under its statutory authority, take action against a Web site if it violates a posted privacy policy.³ The legislation recently recommended by the Commission would give individuals notice about what will be done with information they provide about themselves at the time that it is collected. As indicated below, staff found that currently only a minority of genealogy sites provide notice concerning information provided about others. Similarly, the recommended legislation would ensure that consumers have the right to choose how their personally identifiable information is shared, and to correct any information that is posted about them on a Web site. To the extent that these Web sites are commercial in nature, the FTC would have jurisdiction under the recommended legislation.

GENEALOGY WEB SITES

(1) Dot com Sites

The dot com sites generally sell research software and services and/or allow searches of all their databases for a monthly fee, or allow searches of a sampling of databases for free. A few of the dot com Web sites do post privacy policies, but the focus of these privacy policies is assuring users about the security of their credit card information or e-mail address.

The prominent com sites include myfamily.com (which owns ancestry.com and familyhistory.com) and genealogylibrary.com (which owns familytreemaker.com, genexchange.com, and rootsweb.com). Most of these sites currently provide largely historical data. Only two of the dot com sites (ancestry.com and genexchange.com) post free information about living persons, including names and lineage. Genexchange.com also includes date of birth and place of birth of living individuals.

(2) Dot org Sites

The dot org sites fall into two subcategories—informal and fee-based services. Familysearch.org, associated with the Church of Jesus Christ of Latter-Day Saints, is an informational site and does not charge a fee for searching its databases or for information about how and where to conduct genealogy research. It also offers links to many other Web sites that may be helpful in genealogy research. Other fee-based sites, generally run by volunteers, may be associated with local genealogy organizations or clubs, such as the Ohio Genealogy Society Web site.

(3) Family Web sites

A number of individuals appear to have created family Web sites to record their family trees. These are registered using dot com, dot org, and dot net upper level domains. Many of the dot com Web sites, including rootsweb.com, ancestry.com, onlinefamilytree.com, familytreemaker.com, and family history.com, offer programs that allow users to set up their own personal Web site. Some of the family created Web sites post information about living individuals such as birth records and marriage records (names, place, date), photos of family members, and family reunion information. It appears that the information is provided by related parties. Finally, many of the family operated Web sites require passwords to edit the information or to access certain portions of the Web site.

We hope this review is responsive to your question. Please let us know if we can be of any further assistance.

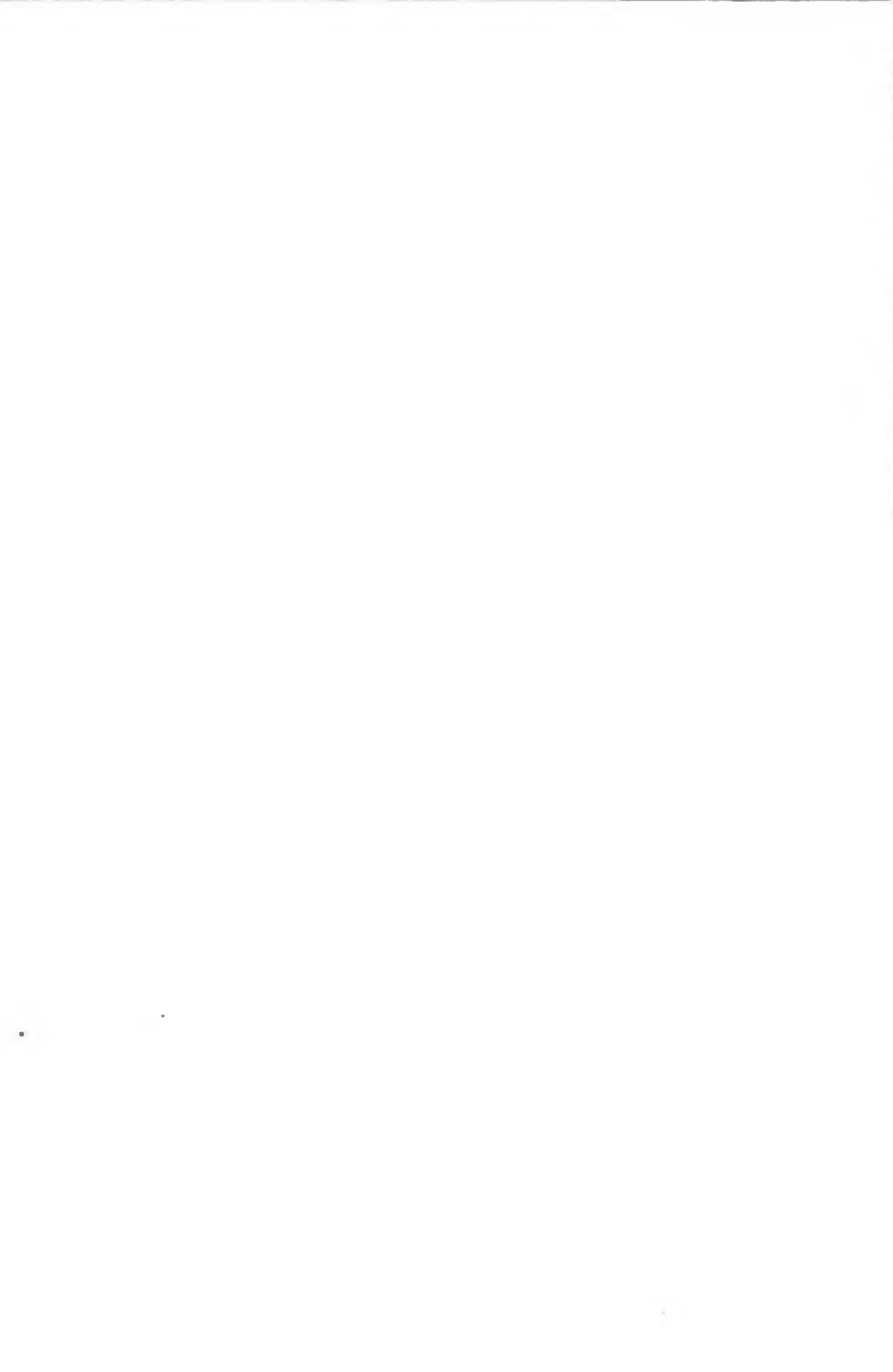
Sincerely,

JODIE BERNSTEIN, *Director.*



²The Children's Online Privacy Protection Act of 1998 protects personal information collected from and about children under thirteen years of age. 15 U.S.C. ss 6501, *et seq.*. The FTC issued regulations implementing the Act on November 3, 1999 (16 C.F.R. Part 312). None of the genealogy sites we visited were directed to children or had areas targeting information collection from children.

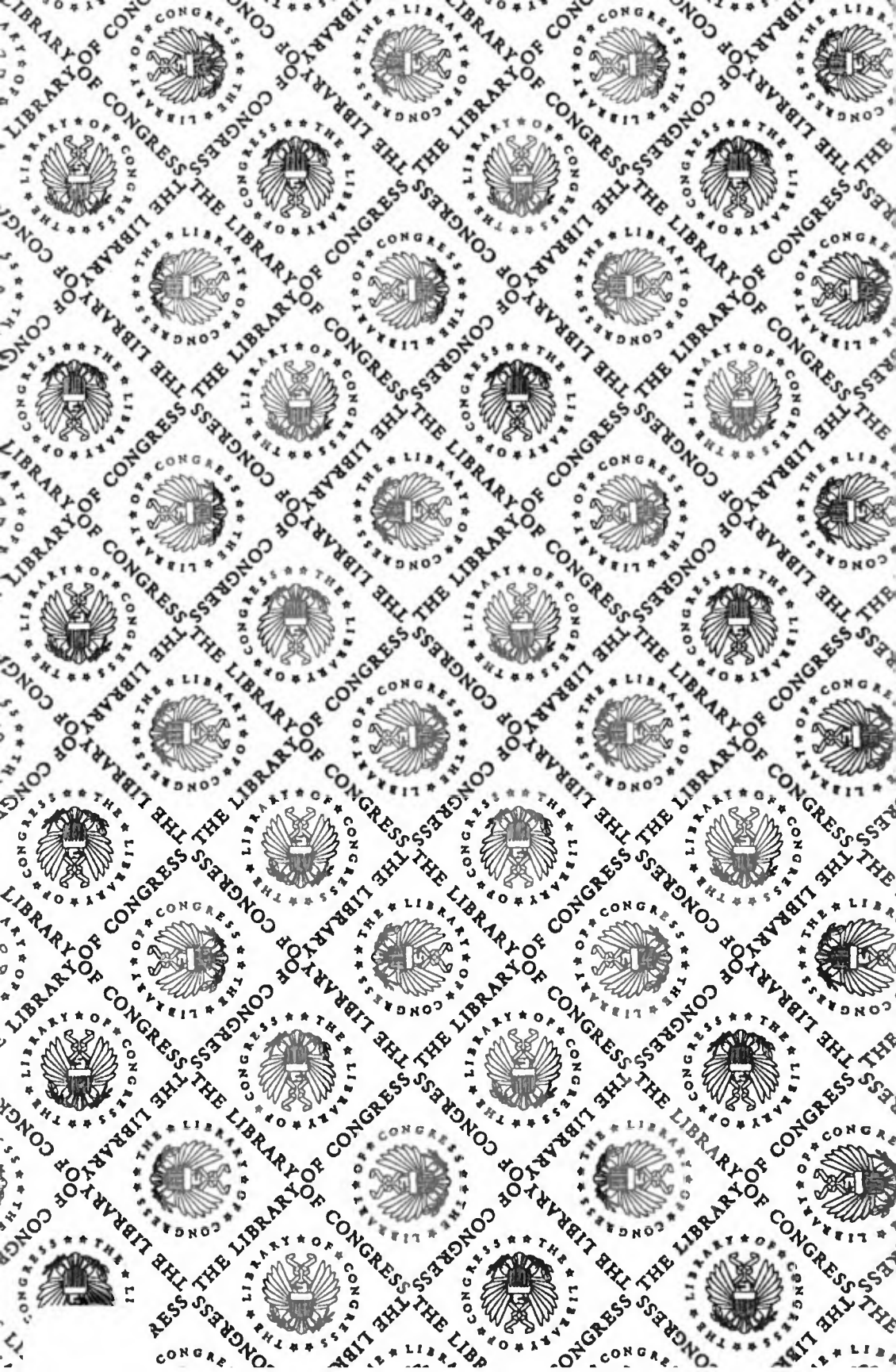
³GeoCities, Docket No. C-3849 (Aug. 1998); *Liberty Financial Companies*, Docket No. C3891 (May. 1999).



LIBRARY OF CONGRESS



0 007 232 548 5



HECKMAN

BINDERY, INC.

Demond-To-Please

03-T1797

N. MANCHESTER, INDIANA 46962

LIBRARY OF CONGRESS



0 007 232 548 5

